



## **Cisco IP Solution Center MPLS VPN 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



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)



## **About This Guide   xi**

Objective	<b>xi</b>
Audience	<b>xi</b>
Organization	<b>xi</b>
Related Documentation	<b>xiii</b>
Obtaining Documentation	<b>xiv</b>
Cisco.com	<b>xiv</b>
Product Documentation DVD	<b>xiv</b>
Ordering Documentation	<b>xiv</b>
Documentation Feedback	<b>xv</b>
Cisco Product Security Overview	<b>xv</b>
Reporting Security Problems in Cisco Products	<b>xv</b>
Obtaining Technical Assistance	<b>xvi</b>
Cisco Technical Support & Documentation Website	<b>xvi</b>
Submitting a Service Request	<b>xvii</b>
Definitions of Service Request Severity	<b>xvii</b>
Obtaining Additional Publications and Information	<b>xvii</b>

---

## **CHAPTER 1**

### **Getting Started with MPLS VPN   1-1**

Before You Begin	<b>1-1</b>
MPLS Service Activation	<b>1-1</b>
Provider Information	<b>1-2</b>
Customer Information	<b>1-2</b>
Resource Information	<b>1-3</b>
Creating CERCs	<b>1-3</b>
Creating VPNs	<b>1-3</b>

---

## **CHAPTER 2**

### **Provisioning Unmanaged Multi-VRF CE   2-1**

Unmanaged MVRFCE Overview	<b>2-1</b>
Process Overview	<b>2-2</b>
Network Inventory	<b>2-2</b>
Service Policy	<b>2-4</b>
Service Request	<b>2-4</b>
MVRFCE PE-CE Policy Type	<b>2-4</b>

Adding New Customer CPE	2-5
Overview of ISC Customers	2-5
Creating Devices	2-6
Creating Logical Devices	2-6
Collecting Configurations	2-8
Monitoring Task Logs	2-10
Creating Customers, Sites, and CPEs	2-10
Creating Customers	2-10
Creating Sites	2-10
Creating CPEs	2-11
Creating New Provider PE	2-12
Overview of ISC Providers	2-13
Creating Device Groups	2-14
Creating Providers and PEs	2-14
Creating Region for PE	2-14
Editing PEs	2-15
Creating Access Domains	2-15
Overview of Access Domains	2-16
Creating Access Domains	2-17

## CHAPTER 3

### Creating Resource Pools 3-1

Overview of Resource Pools	3-1
Create an IP Address Pool	3-2
Create a Multicast Pool	3-4
Create a Route Distinguisher Pool	3-6
Create a Route Target Pool	3-7
Create a Site of Origin Pool	3-9
Create a VC ID Pool	3-11
Create a VLAN Pool	3-13

## CHAPTER 4

### Defining VPNs and CERCs 4-1

Creating MPLS VPN	4-1
Creating IP Multicast VPN	4-3
Creating CE Routing Communities	4-6

## CHAPTER 5

### MPLS VPN Service Policies 5-1

Service Policy Overview	5-1
Creating MPLS VPN in ISC	5-1

Creating Service Policies	5-6
Service Policy Editor	5-6
About IP Addresses in Cisco ISC	5-7
Creating MPLS Service Policy for PE-to-CE Link	5-7
Specifying PE and CE Interface Parameters	5-8
Specifying IP Address Scheme	5-12
Using Existing Loopback Interface Number	5-14
Specifying Routing Protocol for a Service	5-15
Redistribution of IP Routes	5-15
CSC Support	5-15
Giving Only Default Routes to CE	5-15
Static Protocol Chosen	5-16
RIP Protocol Chosen	5-17
BGP Protocol Chosen	5-21
OSPF Protocol Chosen	5-24
EIGRP Protocol Chosen	5-28
None Chosen: Cable Services	5-33
Defining an MVRFC PE-CE Service Policy	5-34
Defining the Service Policy VRF and VPN Information	5-39

## CHAPTER 6

<b>MPLS VPN Service Requests</b>	<b>6-1</b>
Overview of Service Requests	6-1
Service Request Transition States	6-1
Service Enhancements	6-4
How ISC Accesses Network Devices	6-4
Creating Service Requests	6-5
MPLS VPN Topology Example	6-5
Creating a PE-CE Service Request	6-6
Static Routing Protocols	6-14
Creating a Multi-VRF Service Request	6-17
Multi-VRF Overview	6-17
Creating an Multi-VRFCE PE-CE Service Request	6-17
Creating a PE-Only Service Request	6-26
Adding a CLE Service Request	6-33
Deploying Service Requests	6-33
Monitoring Service Requests	6-35
Auditing Service Requests	6-37
Functional Audit	6-37
How to Perform a Functional Audit	6-37

Where to Find the Functional Audit	6-37
Why a Functional Audit Could Fail	6-38
Configuration Audit	6-38
How to Perform a Configuration Audit	6-38
Where to Find the Configuration Audit	6-38
Why a Configuration Audit Could Fail	6-39
Editing Configuration Files	6-39

## CHAPTER 7

### Provisioning Regular PE-CE Links 7-1

MPLS VPN PE-CE Link Overview	7-1
Network Topology	7-2
Prerequisite Tasks	7-2
Infrastructure Data	7-3
Defining a VPN for the PE-CE Link	7-3
Creating MPLS VPN PE-CE Service Policies	7-5
PE-CE Service Policy Overview	7-5
Creating a PE-CE Service Policy	7-6
Creating a PE-NoCE Service Policy	7-10
Creating MPLS VPN PE-CE Service Requests	7-14
Creating a PE-CE Service Request	7-14
Creating a PE-NoCE Service Request	7-21

## CHAPTER 8

### Provisioning MVRFCE PE-CE Links 8-1

MPLS VPN MVRFCE PE-CE Link Overview	8-1
Network Topology	8-2
Prerequisite Tasks	8-3
Infrastructure Data	8-3
Defining a VPN for the MVRFCE PE-CE Link	8-4
Creating MPLS VPN MVRFCE PE-CE Service Policies	8-6
Creating a MVRFCE PE-CE Service Policy	8-6
Creating a PE-NoCE Service Policy	8-12
Creating MPLS VPN MVRFCE PE-CE Service Requests	8-18
Creating a MVRFCE PE-CE Service Request	8-18
Creating a MVRFCE PE-NoCE Service Request	8-27

## CHAPTER 9

### Provisioning Management VPN 9-1

Overview of the ISC Management Network	9-1
Unmanaged Customer Edge Routers	9-1

Managed Customer Edge Routers	9-2
Network Management Subnets	9-3
Issues Regarding Access to VPNs	9-4
Implementation Techniques	9-4
Management CE (MCE)	9-4
Management PE (MPE)	9-5
Management VPN	9-5
Advantages	9-6
Out-of-Band Technique	9-7
Provisioning a Management CE in ISC	9-7
Defining a CE as an MCE	9-8
Creating an MCE Service Request	9-9
Adding PE-CE Links to the Management VPN	9-16

---

**CHAPTER 10**
**Provisioning Cable Services 10-1**

Overview of MPLS VPN Cable	10-1
Benefits of Cable MPLS VPNs	10-1
The Cable MPLS VPN Network	10-2
Management VPN in the Cable Network	10-4
Cable VPN Configuration Overview	10-4
Cable VPN Interfaces and Subinterfaces	10-5
Provisioning Cable Services in ISC	10-6
Creating the Service Requests	10-6
Creating a Cable Subinterface Service Request	10-6
Creating a Cable Link Service Request	10-11

---

**CHAPTER 11**
**Provisioning Carrier Supporting Carrier 11-1**

Carrier Supporting Carrier Overview	11-1
Backbone Network with a Customer Carrier Who Is an ISP	11-1
Backbone Network with a Customer Carrier Who Is a BGP/MPLS VPN Service Provider	11-3
ISC Configuration Options	11-4
LDP/IGP	11-4
IPv4 BGP Label Distribution	11-4
Defining a CSC Service Policy	11-5
Provisioning a CSC Service Request	11-5

---

**CHAPTER 12**
**Provisioning Multiple Devices 12-1**

NPC Ring Topology	12-1
-------------------	------

Ring Topology Overview	12-1
Creating a Ring of Three PE-CLE	12-2
Configuring NPC Ring Topology	12-4
Ethernet-To-The-Home	12-9
ETTH Overview	12-9
Access Domain Management	12-11
ISC ETTH Implementation	12-11
Configuring ETTH	12-11
Residential Service	12-15
Policy for Residential Services Over Shared VLAN	12-16
Service Requests	12-17

## CHAPTER 13

### Spanning Multiple Autonomous Systems 13-1

Overview	13-1
Benefits	13-2
Routing Between Autonomous Systems	13-2
Exchanging VPN Routing Information	13-4
Routing Between Subautonomous Systems in a Confederation	13-8
Using ISC to Span Multiple Autonomous Systems	13-10

## CHAPTER 14

### Generating MPLS Reports 14-1

Overview	14-1
Accessing MPLS Reports	14-1
MPLS PE Service Report	14-3
Running Reports	14-4
MPLS Service Request Report	14-5
Creating Custom Reports	14-6

## APPENDIX A

### IP Solution Center—MPLS VPN A-1

IP Solution Center Overview	A-1
Business Application	A-1
System Architecture	A-2
Load Balancing	A-5
System Features	A-7
Template Manager	A-9
Role-Based Access Control (RBAC)	A-10
North Bound Interface (NBI)	A-10
Service Provider Network	A-12

Resource Pools	<b>A-15</b>
VPN Profile	<b>A-16</b>
Customer View	<b>A-16</b>
Provider View	<b>A-17</b>
Provider Edge Routers	<b>A-18</b>
Multi-VRF CE	<b>A-18</b>
Service Audit	<b>A-19</b>
MPLS VPN	<b>A-20</b>
Intranets and Extranets	<b>A-22</b>
VPN Routing and Forwarding Tables	<b>A-22</b>
VRF Implementation	<b>A-23</b>
VRF Instance	<b>A-24</b>
Route Distinguishers and Route Targets	<b>A-24</b>
Route Target Communities	<b>A-25</b>
CE Routing Communities	<b>A-25</b>
MPLS VPN Security	<b>A-27</b>
Address Space and Routing Separation	<b>A-27</b>
Address Space Separation	<b>A-27</b>
Routing Separation	<b>A-27</b>
Hiding the MPLS Core Structure	<b>A-28</b>
Resistance to Attacks	<b>A-28</b>
Securing the Routing Protocol	<b>A-29</b>
Label Spoofing	<b>A-30</b>
Securing the MPLS Core	<b>A-31</b>
Trusted Devices	<b>A-31</b>
PE-CE Interface	<b>A-31</b>
Routing Authentication	<b>A-32</b>
Separation of CE-PE Links	<b>A-32</b>
LDP Authentication	<b>A-32</b>
Connectivity Between VPNs	<b>A-32</b>
MP-BGP Security Features	<b>A-33</b>
Security Through IP Address Resolution	<b>A-34</b>
Ensuring VPN Isolation	<b>A-34</b>

**APPENDIX B****Service Request Transition States B-1****APPENDIX C****Troubleshooting MPLS VPN C-1**MPLS VPN Provisioning Workflow **C-1**Terms Defined **C-2**

General Troubleshooting Guidelines	<b>C-2</b>
Common Provisioning Issues	<b>C-2</b>
Troubleshooting MPLS VPN and Layer 2 VPN	<b>C-4</b>
Frequently Asked Questions	<b>C-5</b>
Troubleshooting IPsec Mapping into MPLS	<b>C-6</b>

---

**INDEX**



## About This Guide

---

### Objective

This guide describes how to use Cisco IP Solution Center (ISC) to configure and provision Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). This guide explains the concepts, tasks, and screen information that you need to set up the MPLS VPN network infrastructure in ISC and deploy the MPLS VPN service on the network.

### Audience

This guide is designed for network engineers, service operators, and business managers who are responsible for configuring, provisioning, and managing MPLS VPN services on a network. Users of this documentation should be familiar with the following content:

- Basic concepts and terminology used in internetworking
- MPLS VPN terms and technology
- IP Network topologies and protocols

### Organization

This guide contains the following chapters:

Title	Description
Getting Started with MPLS VPN	Describes the tasks required to get started using Cisco IP Solution Center (ISC) Multiprotocol Label Switching (MPLS) virtual private network (VPN).
Provisioning Unmanaged Multi-VRF CE	Describes how to use the Inventory Manager and ISC GUI to implement unmanaged Multi-VRF CE from Device set up to Service Request.
Creating Resource Pools	Describes how to create Resource Pools using the Cisco IP Solution Center (ISC) GUI.

<b>Title</b>	<b>Description (continued)</b>
Defining VPNs and CERCs	Describes how to define MPLS VPNs, IP Multicast VPNs, and CE Routing Communities (CERCs).
MPLS VPN Service Policies	Describes the Policy Manager GUI and work flow for MPLS VPN.
MPLS VPN Service Requests	Describes the Service Requests GUI and work flow for MPLS VPN.
Provisioning Regular PE-CE Links	Describes an end-to-end scenario for creating a Regular PE-CE link.
Provisioning MVRFCE PE-CE Links	Describes an end-to-end scenario for creating an MVRFCE PE-CE link.
Provisioning Management VPN	Describes how to provision a management VPN in ISC.
Provisioning Cable Services	Describes how to provision MPLS VPN cable services.
Provisioning Carrier Supporting Carrier	Describes how to provision Carrier Supporting Carrier.
Provisioning Multiple Devices	Describes how to provision Ethernet to the Home, Hub and Spoke, and Ring Topologies.
Spanning Multiple Autonomous Systems	Describes the network configuration for Spanning Multiple Autonomous Systems.
Generating MPLS Reports	Describes how to create custom MPLS reports.
IP Solution Center—MPLS VPN	Describes an overview of the Cisco IP Solution Center (ISC) Multiprotocol Label Switching (MPLS) virtual private network (VPN) system solution.
Service Request Transition States	Describes the ISC Service Request Transition States.
Troubleshooting MPLS VPN	Describes how to troubleshoot MPLS VPN.

# 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](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](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](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](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](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](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](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](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](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](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](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](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](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](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](mailto: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](mailto: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](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](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](mailto: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](mailto: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](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 MPLS VPN

---

This chapter describes the tasks required to get started using Cisco IP Solution Center (ISC) Multiprotocol Label Switching (MPLS) virtual private network (VPN).

For more information about where MPLS VPN fits into the ISC solution, see Appendix A, “IP Solution Center—MPLS VPN.”

- Before You Begin, page 1-1
- MPLS Service Activation, page 1-1

## Before You Begin

Before you can use MPLS VPN to provision, you must do the following:

---

**Step 1** Install ISC.

See *Cisco IP Solution Center Installation Guide, 4.1*

**Step 2** Purchase the license.

**Step 3** Assess your network.

For example, the network must meet certain criteria such as MPLS, MP-BGP enabled, PE routers in supported platforms, and so forth. ISC provisions only PE-CEs, not devices within a given network.

**Step 4** Populate ISC.

See *Cisco IP Solution Center Infrastructure Reference, 4.1*

---

## MPLS Service Activation

To activate MPLS services you must configure ISC so it “knows” about the preconfiguration information, such as devices, providers, customers, and so on, that ISC is going to manage and their roles.

How to create the associated elements in ISC is explained in the chapter, Service Inventory—Inventory and Connection Manager, and how to discover devices is explained in the chapter, Service Inventory—Discovery, in *Cisco IP Solution Center Infrastructure Reference, 4.1* ([http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4\\_1/infrastr/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/infrastr/index.htm)).

The major steps to achieve MPLS service activation include setting up:

- Provider information – devices, providers, regions, and PEs.
- Customers and Customer Sites.
- CPEs.
- Resource Pools.
- Defining NPC (Named Physical Circuits).

## Provider Information

---

### Step 1 Acquire devices.

There are three ways to bring the devices into ISC:

- Using the ISC Auto-Discovery tool, which will discover the devices. The connections between the devices are populated into the database. The Auto-Discovery tool is located in the Inventory Manager.
- Using the Inventory Manager for bulk-upload and bulk-changes to the database. The Inventory Manager is located in: **Service Inventory > Inventory and Connection Manager > Inventory Manager**.
- Using the ISC main GUI to define a device and doing a Configuration Collection.

### Step 2 Create Provider.

This is a logical container to hold configurations for autonomous systems.

Go to **Service Inventory > Inventory and Connection Manager > Providers**.

### Step 3 Create Regions.

These are logical dividers used to organize PE devices.

Go to **Service Inventory > Inventory and Connection Manager > Providers > Provider Regions**.

### Step 4 Create PEs.

Use “acquired” devices to group into PEs.

Go to **Service Inventory > Inventory and Connection Manager > Providers > PE Devices**.

Define the PE-POPs (n-PE) and PE-CLEs (u-PE) for each region.



---

**Note** For L2 access, you must specify NPE—physical.

---

## Customer Information

---

### Step 1 Create Customers.

These are virtual placeholders for VPN deployment.

Go to **Service Inventory > Inventory and Connection Manager > Customers**.

### Step 2 Create Customer Sites.

- Go to **Service Inventory > Inventory and Connection Manager > Customers > Customer Sites**.
- Step 3** If CEs are to be managed, Create CEs.
- Go to **Service Inventory > Inventory and Connection Manager > Customers > CPE Devices**.
- 

## Resource Information

Resource Pools are used by ISC to automatically assign critical parameters like VLAN, VCID and IP Addresses during the service provisioning.

Go to **Service Inventory > Inventory and Connection Manager > Resource Pools**.

- IP addresses – ISC can auto-assign IP addresses.
    - IP address pools that are tied to Regions.
    - IP address pools are used by ISC to automatically assign IP addresses for PE-CE connections in MPLS L3VPNs. The pool is irrelevant for L2VPNs. IP address pools with /32 pool mask are used for loopbacks on CE; pools with /30 are used for the connection between PEs and CEs.
  - Route Target (RT) Pool:
    - RT pool is critical for a VPN. It is tied to a Provider. ISC uses RT pool to automatically assign RTs in MPLS VPN.
    - ISC can auto-assign this pool.
    - This pool is irrelevant for L2VPNs.
  - Route Distinguisher (RD) Pool:
    - RD pool is tied to a Provider. It is used by VPN to distinguish routes. ISC uses RD pool to automatically assign RDs in MPLS VPN.
    - ISC can auto-assign this pool.
    - This pool is irrelevant for L2VPNs.
  - Site of Origin (SOO) – (optional) ISC can auto-assign these values.
- 

## Creating CERCs

CE Routing Communities (CERCs) is how ISC handles the Route Targets (RT) transparently from the users and it can help the service providers to easily implement various kinds of VPN topology.

Go to **Service Inventory > Inventory and Connection Manager > CE routing Communities**.

## Creating VPNs

VPNs must be created for MPLS VPN services. VPN is just a placeholder where you can tie all different CERCs together to form a complex VPN topology.

Go to **Service Inventory > Inventory and Connection Manager > VPNs**.





## Provisioning Unmanaged Multi-VRF CE

---

This chapter describes how to implement a new, Unmanaged Multi-VPN routing and forwarding tables (MVRF) CE with all the required infrastructure data, define an MVRFCE PE-CE Service Policy, and create an MVRFCE PE-CE Service Request, using the Cisco IP Solution Center (ISC).

This chapter contains the following major sections:

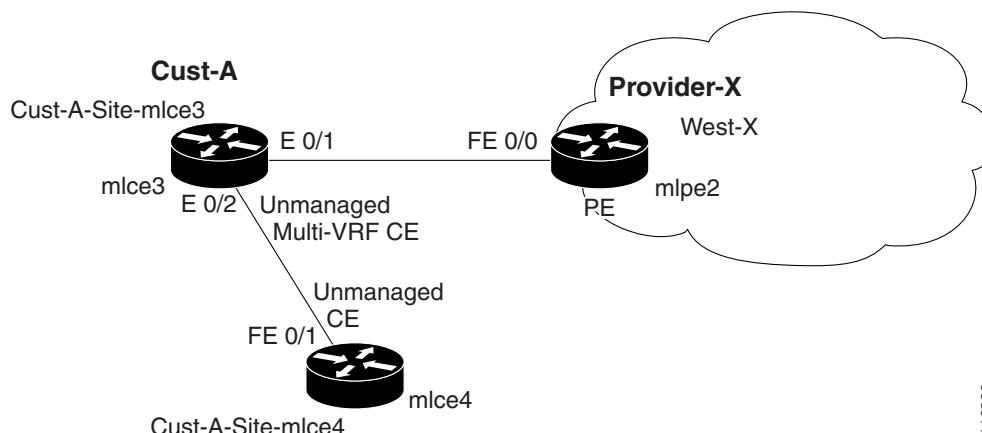
- Unmanaged MVRFCE Overview, page 2-1
- Adding New Customer CPE, page 2-5
- Creating New Provider PE, page 2-12
- Creating Access Domains, page 2-15

### Unmanaged MVRFCE Overview

The unmanaged MVRFCE feature is similar to the unmanaged CE feature in so far as the service provider does not use ISC to upload or download configurations to the CPE. This feature is similar to the managed MVRFCE feature in so far as ISC creates a link with three devices: a PE, an MVRFCE, and a CE.

In the unmanaged scenarios, the customer configures the CPE manually. To automate the process of configuring the unmanaged MVRFCE, the service provider can use ISC to generate the configuration and then send it to the customer for manual implementation.

Figure 2-1 shows an overview of a network topology with MPLS VPN MVRFCE PE-CE links.

**Figure 2-1 Unmanaged MVRFCE PE-CE Network Topology**

The network topology in Figure 2-1 shows a service provider (**Provider-X**) and a customer (**Cust-A**). The Provider contains one Region (**West-X**) and one PE (**mlpe2**). The Customer contains an MVRFCE (**mlce3**) and a CE (**mlce4**). Both of these CPEs are unmanaged.

This section contains the following sections:

- Process Overview, page 2-2
- MVRFCE PE-CE Policy Type, page 2-4

## Process Overview

To configure MPLS VPN services with ISC, you must understand three key concepts:

- Network Inventory, page 2-2
- Service Policy, page 2-4
- Service Request, page 2-4

## Network Inventory

The purpose of preparing network inventory in ISC is to populate the Repository with infrastructure data. If multiple devices are involved, you can use Inventory Manager for importing devices and creating PE or CPE. Otherwise, you can use Inventory and Connection Manager to create the devices and infrastructure data.

To create an MPLS VPN Service Request, you must create the following infrastructure data:

- Devices

A Device in ISC is a logical representation of a physical device in the network. You can import devices (configurations) into ISC by using Inventory Manager or the ISC GUI. You can also use the Auto Discovery feature of Inventory Manager to import devices into the Repository.

- Customers

A customer is typically an enterprise or large corporation that receives network services from a service provider. A Customer is also a key logical component of ISC.

- Sites

A Site is a logical component of ISC that connects a Customer with a CE. It can also represent a physical customer site.

- CPE/CE Devices

A CPE is “customer premises equipment,” typically a customer edge router (CE). It is also a logical component of ISC. You can create CPE in ISC by associating a device with a Customer Site.

- Providers

A provider is typically a “service provider” or large corporation that provides network services to a customer. A Provider is also a key logical component of ISC.

- Regions

A Region is a logical component of ISC that connects a Provider with a PE. It can also represent a physical provider region.

- PE Devices

A PE is a provider edge router or switch. It is also a logical component of ISC. You can create PE in ISC by associating a Device with a Provider Region. In ISC, a PE can be a “point of presence” router (POP) or a Layer 2 switch (CLE).

- Access Domains (for Layer 2 Access)

The Layer 2 Ethernet switching domain that connects a PE to a CE is called an Access Domain. All the switches attached to the PE-POP belong to this Access Domain. These switches belong to the Provider and are defined in ISC as PE-CLE.

- Resource Pools

- IP Addresses
  - Multicast
  - Route Distinguisher
  - Route Target
  - VLANs (for Layer 2 Access)

- CE Routing Communities (CERC is optional)

- VPN

Before creating a Service Policy, a VPN name must be defined within ISC.

## Service Policy

To create an MVRFCE PE-CE Service Policy (see Chapter 5, “MPLS VPN Service Policies”), you must set up the following items:

1. Policy Type
2. PE-MVRFCE Interface
3. MVRFCE-CE Interface
4. PE-MVRFCE IP Address Scheme
5. MVRFCE-CE IP Address Scheme
6. PE-MVRFCE Routing Information
7. MVRFCE-CE Routing Information
8. VRF and VPN Membership

## Service Request

To create an MVRFCE PE-CE Service Request (see Chapter 6, “MPLS VPN Service Requests”), you must complete the following items:

1. PE-MVRFCE Interface
2. MVRFCE-CE Interface
3. PE-MVRFCE IP Address Scheme
4. MVRFCE-CE IP Address Scheme
5. PE-MVRFCE Routing Information
6. MVRFCE-CE Routing Information
7. VRF and VPN Membership

## MVRFCE PE-CE Policy Type

An MVRFCE PE-CE Policy Type is a PE to CE link with three devices:

- PE
- MVRF CE
- CE

Figure 2-2 shows an example of an MVRFCE PE-CE link with three devices.

**Figure 2-2** MVRFCE PE-CE Link



In an MVRFCE PE-CE Service Policy with CE Present enabled, interfaces FE 0/0, E 0/1, E 0/2 and FE 0/1 are configured as an MPLS VPN link in the Service Request process.

# Adding New Customer CPE

This section describes how to create a new CPE with an Unmanaged Multi-VRF management Type using the Cisco IP Solution Center (ISC) GUI. It contains the following sections:

- Overview of ISC Customers, page 2-5
- Creating Devices, page 2-6
- Creating Customers, Sites, and CPEs, page 2-10

## Overview of ISC Customers

In ISC, a Customer is defined by the following three logical components:

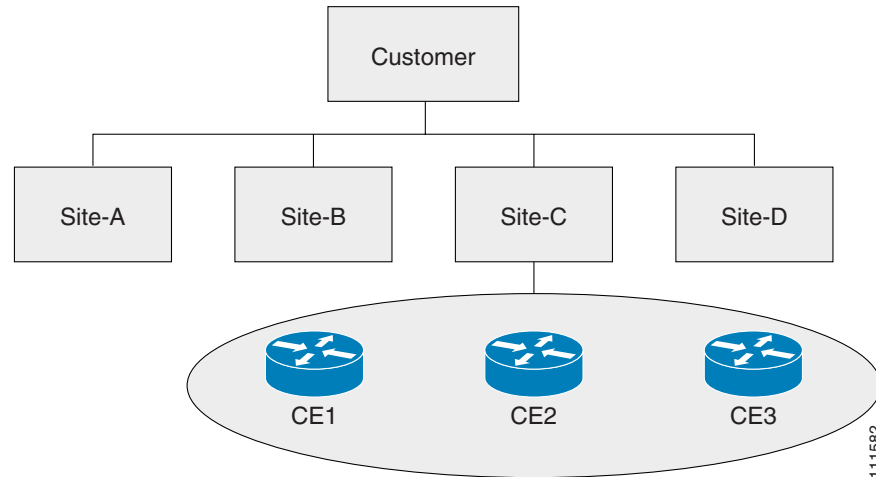
- Customer Name
- Customer Site
- Customer Device (CPE)

In ISC, a Customer is a logical container for Sites and CEs.

Within a Customer, there can be one or more Sites. Sites are logical entities that can be defined in any way that makes sense to a service provider.

Figure 2-3 shows an overview of an ISC Customer.

**Figure 2-3** Overview of an ISC Customer



## Creating Devices

This section describes how to create a Device with the ISC GUI, connect to a Cisco IOS router in the network, collect the live configuration, and populate the Repository. This section contains the following sections:

- Creating Logical Devices, page 2-6
- Collecting Configurations, page 2-8
- Monitoring Task Logs, page 2-10

### Creating Logical Devices

- 
- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Devices**.  
The Devices window appears.
- Step 3** Click **Create**.
- Step 4** From the drop-down list, choose **Cisco Device**.  
The Create Cisco Device window appears (see Figure 2-4).

**Figure 2-4 New Device Information**

**Create Cisco Device**

General	
Device Host Name * :	<input type="text"/>
Device Domain Name:	<input type="text"/>
Description:	<input type="text"/>
Collection Zone:	None ▾
Management IP Address:	<input type="text"/>
Interfaces:	<input type="button" value="Edit"/>
Associated Groups	<input type="button" value="Edit"/>
Login and Password Information	
Login User:	<input type="text"/>
Login Password:	<input type="text"/>
Verify Login Password:	<input type="text"/>
Enable User:	<input type="text"/>
Enable Password:	<input type="text"/>
Verify Enable Password:	<input type="text"/>
Device and Configuration Access Information	
Terminal Session Protocol:	Default (Telnet) ▾
Config Access Protocol:	Default (Terminal) ▾
OS:	IOS ▾
SNMP Version:	Default (SNMP v1/v2c) ▾
SNMP v1/v2c	
Community String RO:	<input type="text"/>
Community String RW:	<input type="text"/>
Additional Properties:	<input type="button" value="Show"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Note: \* - Required Field

149136

**Step 5** Enter all required information for this new device.

**Step 6** For Additional Properties, click **Show**.

**Step 7** To save this new device, click **Save**.

You have saved a Device in the Repository.

Collecting Configurations

This section describes how to connect to the physical device in the network, collect the device information from the router, and populate the Repository.

- Step 1

Go to **Monitoring > Task Manager**.  
The Tasks window appears.
- Step 2

Click **Create**.
- Step 3

Choose **Collect Config**.  
The Create Task window appears, as shown in Figure 2-5.



**Tip** You might want to change the default **Name** and **Description** for this task, so you can more easily identify it in the task log.

Figure 2-5 Create Task

Create Task

Name*:	Collect Config 2004-01-14 (mlce3DeviceCreation)
Type:	Collect Config
Description:	Created on 2004-01-14 mlce3DeviceCreation
Task Configuration Method:	<input checked="" type="radio"/> Simplified <input type="radio"/> Advanced (via wizard)

Note: \* - Required Field

111575

- Step 4

Click **Next**.  
The Collect Config Task window appears, as shown in Figure 2-6.

**Figure 2-6 Collect Config Task**

**Collect Config Task**

Collect Config Task:Collect Config 2004-01-14 (mlce3DeviceCreation)

**Devices:** Select/De Select

**Groups:** Select/De Select

**Options:**

- ☒ Retrieve device attributes
- ☒ Retrieve Interfaces

**Schedule:**

- ☒ Now
- ☐ Later
- ☐ None

**Task Owner:**

- ☐ Customer
- ☐ Provider
- ☒ None

Submit Cancel

Note: \* - Required Field

111576

- Step 5** To choose devices associated to the task, in the Devices panel, click **Select/De Select**.  
The Choose Device window appears.
- Step 6** Check to choose the desired device(s), then click **Select**.  
The Collect Config Task window reappears.  
To Choose device groups associated to the task, in the Groups panel, click **Select/De Select**.  
A list of available device groups appears.
- Step 7** Check to choose the desired device group(s), then click **Select**.  
The Collect Config Task window reappears.
- Step 8** Set schedule and task owner, if applicable.
- Step 9** Click **Submit**.  
The Tasks window appears.
- Step 10** Choose your task in the Task Name column, then click **Details** to view more information.

## Monitoring Task Logs

---

**Step 1** Go to **Monitoring > Task Manager**.

The Tasks window appears.

**Step 2** In the Selection pane, click **Logs**.

The Task Runtime Actions window appears.




---

**Note** The **Status** field shows the task has completed successfully.

---

**Step 3** Choose your task and then click **Instances** to view more information.

---

## Creating Customers, Sites, and CPEs

This section describes how to create a Customer with the ISC GUI, create a Site for the Customer, and associate a Device with the Site. This section contains the following sections:

- Creating Customers, page 2-10
- Creating Sites, page 2-10
- Creating CPEs, page 2-11

### Creating Customers

---

**Step 1** Go to **Service Inventory > Inventory and Connection Manager > Customers**.

The Customers window appears.

**Step 2** Click **Create**.

The Create Customer window appears.

**Step 3** Enter a Customer Name and then click **Save**.

The Customers window appears.

---

### Creating Sites

---

**Step 1** Go to **Service Inventory > Inventory and Connection Manager**.

**Step 2** In the Selection pane, click **Customer Sites**.

The Customer Site window appears.

**Step 3** Click **Create**.

The Create Customer Site window appears.

- Step 4** Enter a site name in the Name field.
- Step 5** To associate a customer to this site, in the Customer field, click **Select**.  
A list of available customer names appears.
- Step 6** Check to choose the desired customer, then click **Select**.  
The Create Customer Site window reappears.
- Step 7** Click **Save**.
- 

## Creating CPEs

---

- Step 1** Go to **Service Inventory > Inventory and Connection Manager**.
- Step 2** In the Selection pane, click **CPE Devices**.  
The CPE Devices window appears.
- Step 3** Click **Create**.  
The Create CPE Device window appears.
- Step 4** In the Device Name field, click **Select**.  
The Choose Device window appears.
- Step 5** Check to choose a device, then click **Select**.  
The Create CPE Device window reappears, as shown in Figure 2-7.

**Figure 2-7 Create CPE Device**

**Create CPE Device**

Device Name\*: mlce3 Select

Site Name\*: Cust-A-Site-mlce3 Select

Customer Name: Cust-A

Management Type: Unmanaged Multi-VRF

Pre-shared Keys: Edit

Isec High Availability Options: ☒ None ☐ Normal Failover ☐ Stateful Failover

Isec Public IP Address:

IP Address Ranges: Edit

Show Interfaces with: Name Matching: Ethernet\* Find

Showing 1 - 5 of 5 records

#	Interface Name	IP Address	IP Address Type	Encapsulation	Description	Isec	Firewall	NAT	QoS Candidate
1.	Ethernet0/0	172.29.146.26/26	STATIC	ETHERNET		None	None	None	None
2.	Ethernet0/1		STATIC	ETHERNET	Link To MLPE2	None	None	None	None
3.	Ethernet0/1.101	10.10.10.6/30	STATIC	DOT1Q	Ethernet0/1.101 dot1q vlan id=101. By VPNSC: Job Id# = 2	None	None	None	None
4.	Ethernet0/2		STATIC	ETHERNET	Link To MLCE4	None	None	None	None
5.	Ethernet0/3	9.0.0.1/24	STATIC	ETHERNET	Link To MLCE5	None	None	None	None

Rows per page: 10 Go to page: 1 of 1

Save Cancel

Note: \* - Required Field

111570

**Step 6** From the drop-down list, choose a Management Type (**Unmanaged Multi-VRF**).

**Step 7** Click **Save**.

The Create CPE Device window appears showing the Unmanaged Multi-VRF CPE Device you have created.

## Creating New Provider PE

This section contains the following sections:

- Overview of ISC Providers, page 2-13
- Creating Device Groups, page 2-14
- Creating Providers and PEs, page 2-14
- Creating Region for PE, page 2-14
- Editing PEs, page 2-15

## Overview of ISC Providers

In ISC, a Provider is defined by the following three logical components:

- Provider Name and BGP Autonomous System (AS) number
- Provider Region
- Provider Device (PE)

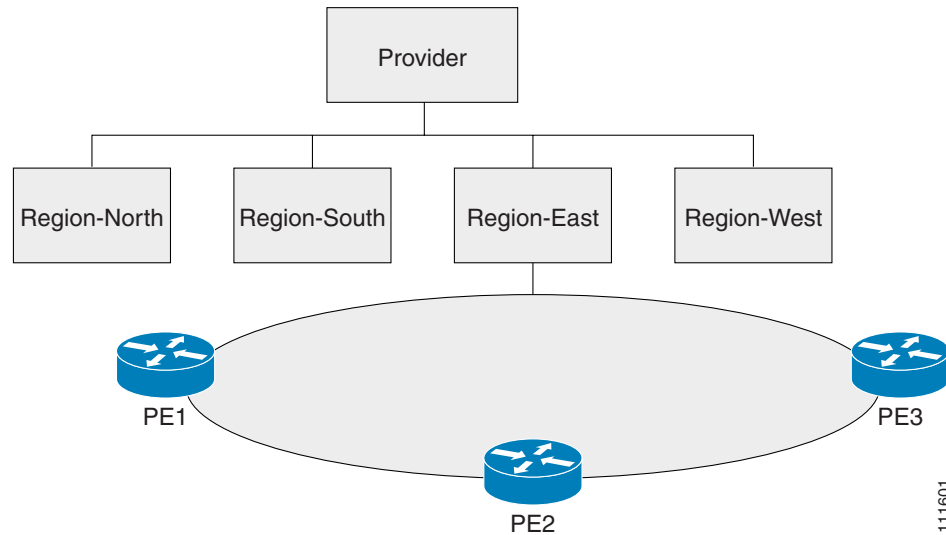
In ISC, a provider administrative domain (PAD) is a single AS. It is not a specific service provider, rather it is a logical container for Regions and PEs.

Within a single PAD, there must be one or more Regions. Regions are logical entities that can be defined in any way that makes sense to a service provider.

Within a Region, a Provider can contain one or more PEs. The PEs can be a PE-POP (“router”) or a PE-CLE (“switch”).

Figure 2-3 shows an overview of an ISC Provider.

**Figure 2-8** Overview of an ISC Provider



## Creating Device Groups

- 
- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Device Groups**.  
The Device Groups window appears.
- Step 3** Click **Create**.  
The Create Device Group window appears.
- Step 4** In the Name field, enter the Device Group Name.
- Step 5** Click **Save**.
- 

## Creating Providers and PEs

- 
- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Providers**.  
The Providers window appears.
- Step 3** Click **Create**.  
The Create Provides window appears.
- Step 4** In the Name field, enter a provider name.
- Step 5** In the BGP AS (Boarder Gateway Protocol Autonomous System) field, enter a a valid value (1-65535).
- Step 6** Enter contact information is applicable.
- Step 7** Click **Save**.
- 

## Creating Region for PE

- 
- Step 1** Log into ISC.
- Step 2** In the Selection pane, click **Provider Regions**.  
The Provider Regions window appears.
- Step 3** Click **Create**.  
The Create Provider Region window appears.
- Step 4** In the Name field, enter a provider region name.
- Step 5** In the Provider field, accept the default value, if one is shown, or to choose a provider, click **Select**.
- Step 6** Click **Save**.
-

## Editing PEs

This section describes how to view or edit a PE with the ISC GUI.

To view a PE with the ISC GUI, follow these steps:

- Step 1** Open a new browser and log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager**.
- Step 3** In the Selection pane, click **PE Devices**.

The PE Devices window appears, as shown in Figure 2-9.

**Figure 2-9 PE Devices**

#	Device Name	Provider Name	Region Name	Role Type	Service Request
1. <input type="checkbox"/>	mlpe3	Provider-X	East-X	PE_POP	

- Step 4** Choose the PE Device.
- Step 5** Click **Edit**.  
The Edit PE Device window appears.
- Step 6** Make required changes, then click **Save**.

## Creating Access Domains



### Note

This section is only required for Layer 2 access to MPLS VPN.

This section describes how to create an Access Domain using the Cisco IP Solution Center (ISC) GUI. This section contains the following sections:

- Overview of Access Domains, page 2-16
- Creating Access Domains, page 2-17

## Overview of Access Domains

Any Transport over MPLS (AToM) is the Cisco solution for transporting Layer 2 traffic over an IP/MPLS backbone. AToM is required for supporting legacy services over MPLS infrastructures and for supporting new connectivity options, including Layer 2 VPNs and Layer 2 virtual leased lines.

AToM supports three types of Ethernet-based L2VPNs (EoMPLS):

- Point-to-Point Ethernet Wire Service (EWS)
- Point-to-Point Ethernet Relay Service (ERS)
- Multipoint TLS Service

The Layer 2 Ethernet switching domain that connects a PE to a CE is called an Access Domain. All the switches attached to the PE-POP belong to this Access Domain. These switches belong to the Provider and are defined in ISC as PE-CLE.

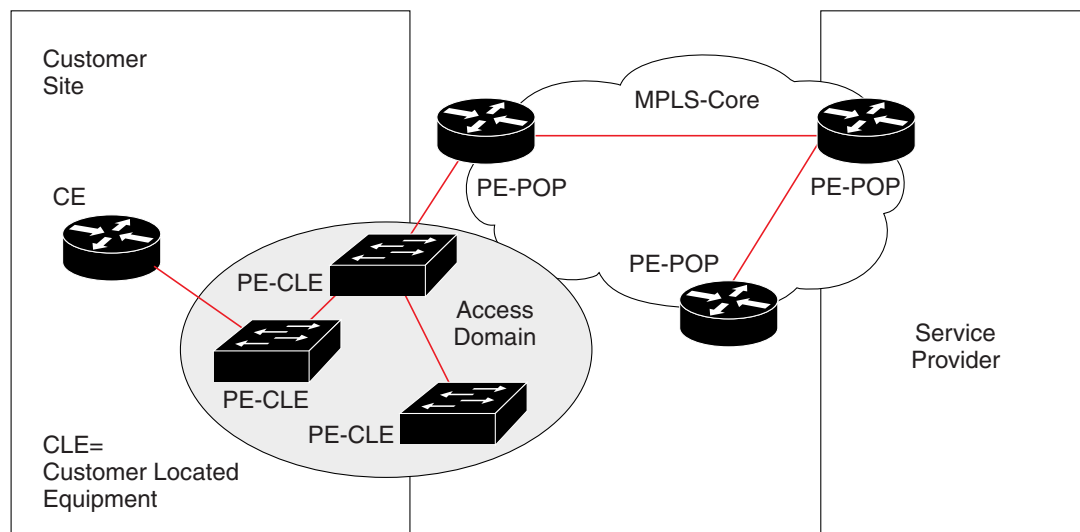
**Note**

To have ISC automatically assign VLAN links from a VLAN pool, you must create an Access Domain.

ISC supports multiple PE-POPs per Access Domain and multiple PE-CLE devices can be included.

Figure 2-10 shows an overview of an ISC Access Domain.

**Figure 2-10** Overview of an Access Domain



111621

## Creating Access Domains

- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager**.
- Step 3** In the Selection pane, under **Providers**, click **Access Domains**.  
The Access Domains window appears.
- Step 4** Click **Create**.  
The Create Access Domain window appears, as shown in Figure 2-11.

**Figure 2-11** Create Access Domain

**Create Access Domain**

Name \*: AD-North-X

Provider \*: Provider-X Select

PEs \*: Select

Reserved VLANs:

#	Start	Size	Management VLAN
Showing 0 of 0 records			

Rows per page: 10 Go to page: 1 of 1 Go ▶▶

Create Edit Delete

Save Cancel

Note: \* - Required Field

- Step 5** Enter an Access Domain Name.
- Step 6** Choose a Provider.
- Step 7** Click **Select** to show PEs.  
The Show PEs window appears.
- Step 8** Choose a PE.
- Step 9** Click **Select**.  
You are returned to the Create Access Domain window.
- Step 10** For Reserved VLNs, click **Create**.  
The Create Reserved VLAN window appears, as shown in Figure 2-12.

**Figure 2-12 Create Reserved VLAN**

Starting Value: *	500	(1 - 4094)
Size: *	100	(1 - 4094)
Management VLAN:	<input checked="" type="checkbox"/>	
<div>OK Cancel</div>		

Note: \* - Required Field

111619

**Step 11** Enter a Starting Value.

**Step 12** Enter a Size.

**Step 13** Choose **Management VLAN**.

**Step 14** Click **OK**.

The Access Domains window appears showing that the Access Domain has been saved in the Repository.



## Creating Resource Pools

This chapter describes how to create Resource Pools using the Cisco IP Solution Center (ISC) GUI.

This chapter contains the following sections:

- Overview of Resource Pools, page 3-1
- Create an IP Address Pool, page 3-2
- Create a Multicast Pool, page 3-4
- Create a Route Distinguisher Pool, page 3-6
- Create a Route Target Pool, page 3-7
- Create a Site of Origin Pool, page 3-9
- Create a VC ID Pool, page 3-11
- Create a VLAN Pool, page 3-13

## Overview of Resource Pools

Before creating a service in ISC, you must define your Resource Pools. From these Resource Pools, ISC can automatically assign some values during the provisioning process. You can also manually assign these values during the provisioning process, but it is not recommended.

ISC allocates numbers from the following pools during the provisioning process:

- **IP Address**—Connects PE and CE interfaces, when you define addresses in a Service Request.
- **Multicast**—Class D addresses used with multicast, when building PE to multiple CE links.
- **Route Distinguisher (RD)**—A 64-bit number composed of the Provider AS number and an index number that is prepended to a VPN route. The RD allows the route subnet to be unique across the entire provider MPLS VPN network. It is carried by MP-BGPv4 as a 96-bit VPNv4 address as part of the extended community string.
- **Route Target (RT)**—An import and export feature of a VRF, the RT allows VPN routes to be forwarded between VRFs. It is a 64-bit number, also carried as part of the MP-BGPv4 extended community string, and directly related to each VPNv4 route and its VPN-related IPv4 route.
- **Site of Origin**—Indicates the origin of a BGP update. Depending on the use of two Cisco IOS BGP commands, the Site of Origin will be used by BGP to preclude routing loops.
- **VC ID (Virtual Circuit)**—Used as a Layer 2 circuit identifier across a provider network.
- **VLAN**—Used in a Layer 2 VPN as a circuit identifier within the provider Access Domain.

# Create an IP Address Pool

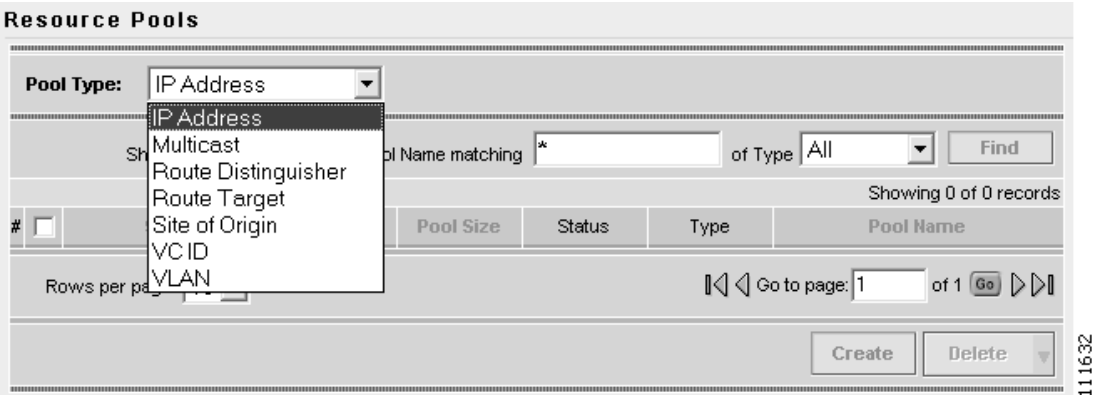
This section describes how to create an IP Address Pool with the ISC GUI.  
To create an IP Address Pool with the ISC GUI, follow these steps:

- Step 1

Log into ISC.
- Step 2

Go to **Service Inventory > Inventory and Connection Manager > Resource Pools**.  
The **Resource Pools** window appears, as shown in Figure 3-1.

Figure 3-1 Resource Pools

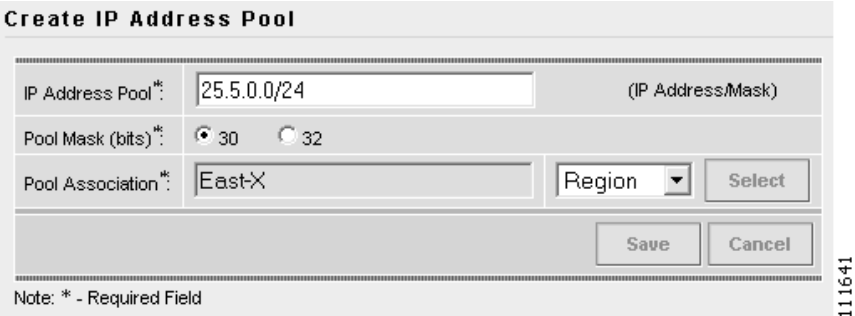


- Step 3

Go to **IP Address** from the Pool Type window.
- Step 4

Click **Create**.  
The Create IP Address Pool window appears, as shown in Figure 3-2.

Figure 3-2 Create IP Address Pool



- Step 5

Enter an *IP Address* and *Mask*. (25.5.0.0/24)
- Step 6

Choose the **Pool Mask (bits)** value. (30)



**Note** Use **32** for loopback addresses.

- Step 7** Click **Select** to associate the pool with a Region.  
The Choose Region window appears, as shown in Figure 3-3.

**Figure 3-3 Choose Region**

Showing 1 - 1 of 1 record

#	Region Name	Provider Name
1.	East-X	Provider-X

Rows per page: 10 Go to page: 1 of 1

Select Cancel

- Step 8** Choose a Region.

- Step 9** Click **Select**.

The Create IP Address Pool window appears, as shown in Figure 3-4.

**Figure 3-4 Create IP Address Pool**

IP Address Pool\*: 25.5.0.0/24 (IP Address/Mask)

Pool Mask (bits)\*: 30 32

Pool Association\*: East-X Region Select

Save Cancel

Note: \* - Required Field

- Step 10** Click **Save**.

The **Resource Pools - IP Address** window appears, as shown in Figure 3-5.

**Figure 3-5      Resource Pools - IP Address**

**Resource Pools**

Pool Type:

Show IP Address Pools with Pool Name matching  of Type

Showing 1 - 1 of 1 record

#	Start	Pool Mask	Pool Size	Status	Type	Pool Name
1.	<input type="checkbox"/> 25.5.0.0	30	62	Available	Region	Provider-X:East-X

Rows per page:   1 of 1

111644

You have saved an IP Address Pool in the Repository.

## Create a Multicast Pool

This section describes how to create a Multicast Address Pool with the ISC GUI.

To create a Multicast Pool with the ISC GUI, follow these steps:

- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Resource Pools**.  
The **Resource Pools** window appears (not shown).
- Step 3** Choose **Multicast** from the **Pool Type** window.  
The **Resource Pools - Multicast** window appears, as shown in Figure 3-6.

**Figure 3-6      Resource Pools - Multicast**

**Resource Pools**

Pool Type:

Showing 0 of 0 records

#	Multicast Address	Size	Use Default MDT	Use Data MDT	Status
---	-------------------	------	-----------------	--------------	--------

Rows per page:   1 of 1

111645

**Step 4** Click **Create**.

The **Create Multicast Pool** window appears, as shown in Figure 3-7.

**Figure 3-7 Create Multicast Pool**

**Create Multicast Pool**

Multicast Address \*: 239.0.0.0/24 (IP Address/Mask)

Use for Default MDT: ☒

Use for Data MDT: ☒

Save Cancel

Note: \* - Required Field

**Step 5** Enter an *IP Address* and *Mask*. (**239.0.0.0/24**)

**Step 6** Choose the defaults. (**Default MDT** and **Data MDT**).

**Step 7** Click **Save**.

The **Resource Pools - Multicast** window appears, as shown in Figure 3-6.

**Figure 3-8 Resource Pools - Multicast**

**Resource Pools**

Pool Type: Multicast

Refresh

Showing 1 - 1 of 1 record

#	Multicast Address	Size	Use Default MDT	Use Data MDT	Status
1.	239.0.0.0	256	true	true	Available

Rows per page: 10

Go to page: 1 of 1

Create Delete

You have saved a Multicast Address Pool in the Repository.

## Create a Route Distinguisher Pool

This section describes how to create a Route Distinguisher Pool with the ISC GUI.

To create a Route Distinguisher Pool with the ISC GUI, follow these steps:

- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Resource Pools**.  
The **Resource Pools** window appears (not shown).
- Step 3** Choose **Route Distinguisher** from the **Pool Type** window.  
The **Resource Pools - Route Distinguisher** window appears, as shown in Figure 3-9.

**Figure 3-9** Resource Pools - Route Distinguisher

Resource Pools

Pool Type: Route Distinguisher

Show Route Distinguisher Pools with Pool Name matching \* Find

Showing 0 of 0 records

#	Start	Pool Size	Status	Pool Name
---	-------	-----------	--------	-----------

Rows per page: 10 Go to page: 1 of 1 Go

Create Delete

111648

- Step 4** Click **Create**.  
The **Create Route Distinguisher Pool** window appears, as shown in Figure 3-10.

**Figure 3-10** Create Route Distinguisher Pool

Create Route Distinguisher Pool

RD Pool Start\*: 0 (0 - 2147483646)

RD Pool Size\*: 0 (1 - 2147483647)

Provider\*: Provider-X Select

Save Cancel

Note: \* - Required Field

111622

- Step 5** Enter an *RD Pool Start*. (**50000**)
- Step 6** Enter an *RD Pool Size*. (**1000**)
- Step 7** Click **Select**.  
The Choose Provider window appears (not shown).

**Step 8** Choose a **Provider**.

The **Create Route Distinguisher Pool** window appears, as shown in Figure 3-11.

**Figure 3-11** Create Route Distinguisher Pool

**Create Route Distinguisher Pool**

RD Pool Start\*: 50000 (0 - 2147483646)

RD Pool Size\*: 1000 (1 - 2147483647)

Provider\*: Provider-X

Note: \* - Required Field

**Step 9** Click **Save**.

The **Resource Pools - Route Distinguisher** window appears, as shown in Figure 3-12.

**Figure 3-12** Create Route Distinguisher Pool

**Resource Pools**

Pool Type: Route Distinguisher

Show Route Distinguisher Pools with Pool Name matching \*

Showing 1 - 1 of 1 record

#	Start	Pool Size	Status	Pool Name
1. <input type="checkbox"/>	50000	1000	Available	99:Provider-X

Rows per page: 10

You have saved a Route Distinguisher Pool in the Repository.

## Create a Route Target Pool

This section describes how to create a Route Target Pool with the ISC GUI.

To create a Route Target Pool with the ISC GUI, follow these steps:

**Step 1** Log into ISC.

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

The **Resource Pools** window appears (not shown).

- Step 3** Choose **Route Target** from the **Pool Type** window.  
The **Resource Pools - Route Target** window appears, as shown in Figure 3-13.

Figure 3-13 Create Route Target Pool

Resource Pools

Pool Type: Route Target

Show Route Target Pools with Pool Name matching \* Find

Showing 0 of 0 records

#	Start	Pool Size	Status	Pool Name
---	-------	-----------	--------	-----------

Rows per page: 10 Go to page: 1 of 1 Go

Create Delete

111625

**Step 4** Click **Create**.  
The **Create Route Target Pool** window appears, as shown in Figure 3-14.

Figure 3-14 Create Route Target Pool

Create Route Target Pool

RT Pool Start \*: 0 (0 - 2147483646)

RT Pool Size \*: 0 (1 - 2147483647)

Provider \*: Provider-X Select

Save Cancel

Note: \* - Required Field

111626

**Step 5** Enter an *RT Pool Start*. (**50000**)  
**Step 6** Enter an *RT Pool Size*. (**1000**)  
**Step 7** Click **Select**.  
The **Choose Provider** window appears (not shown).  
**Step 8** Choose a **Provider**.  
The **Create Route Target Pool** window appears, as shown in Figure 3-15.

Cisco IP Solution Center MPLS VPN User Guide, 4.1

3-8

OL-7646-03

**Figure 3-15 Create Route Target Pool**

**Create Route Target Pool**

RT Pool Start\*: 50000 (0 - 2147483646)

RT Pool Size\*: 1000 (1 - 2147483647)

Provider\*: Provider-X

Note: \* - Required Field

111627

**Step 9** Click **Save**.

The **Resource Pools - Route Target** window appears, as shown in Figure 3-16.

**Figure 3-16 Resource Pools - Route Target**

**Resource Pools**

Pool Type: Route Distinguisher

Show Route Distinguisher Pools with Pool Name matching \*

Showing 1 - 1 of 1 record

#	Start	Pool Size	Status	Pool Name
1.	50000	1000	Available	99:Provider-X

Rows per page: 10

111624

You have saved a Route Target Pool in the Repository.

## Create a Site of Origin Pool

This section describes how to create a Site of Origin Pool with the ISC GUI.

To create a Site of Origin Pool with the ISC GUI, follow these steps:

- 
- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Resource Pools**.  
The **Resource Pools** window appears (not shown).
- Step 3** Choose **Site of Origin** from the **Pool Type** window.  
The **Resource Pools - Site of Origin** window appears, as shown in Figure 3-17.

**Figure 3-17** Resource Pools - Site of Origin

**Resource Pools**

Pool Type: Site of Origin

Show Site of Origin Pools with Pool Name matching \* Find

Showing 0 of 0 records

#	Start	Pool Size	Status	Pool Name
Rows per page: 10 Go to page: 1 of 1 Go				

Create Delete

111629

**Step 4** Click **Create**.

The **Create Site of Origin Pool** window appears, as shown in Figure 3-18.

**Figure 3-18** Create Site of Origin Pool

**Create Site of Origin Pool**

SOO Pool Start\*: 50000 (0 - 2147483646)

SOO Pool Size\*: 1000 (1 - 2147483647)

Provider\*: Provider-X Select

Save Cancel

Note: \* - Required Field

111630

**Step 5** Enter an *SOO Pool Start*. (**50000**)

**Step 6** Enter an *SOO Pool Size*. (**1000**)

**Step 7** Click **Select**.

The Choose Provider window appears (not shown).

**Step 8** Choose a **Provider**.

The Create Route Target Pool window appears, as shown in Figure 3-19.

**Figure 3-19 Resource Pools - Site of Origin**

**Resource Pools**

Pool Type: Site of Origin

Show Site of Origin Pools with Pool Name matching  Find

Showing 1 - 1 of 1 record

#	Start	Pool Size	Status	Pool Name
1.	50000	1000	Available	99:Provider-X

Rows per page: 10 Go to page: 1 of 1 Go

Create Delete

You have saved a Site of Origin Pool in the Repository.

## Create a VC ID Pool

This section describes how to create a Virtual Circuit ID (VC ID) Pool with the ISC GUI.

To create a VC ID Pool with the ISC GUI, follow these steps:

- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Resource Pools**.  
The **Resource Pools** window appears (not shown).
- Step 3** Choose **VC ID** from the **Pool Type** window.  
The **Resource Pools - VC ID** window appears, as shown in Figure 3-20.

**Figure 3-20 Resource Pools - VC ID**

**Resource Pools**

Pool Type: VC ID

Refresh

Showing 0 of 0 records

#	Start	Pool Size	Status
---	-------	-----------	--------

Rows per page: 10 Go to page: 1 of 1 Go

Create Delete

- Step 4** Click **Create**.  
The **Create VC ID Pool** window appears, as shown in Figure 3-21.

Figure 3-21      Create VC ID Pool

Create VC ID Pool

VC Pool Start\*: 50000 (1 - 2147483646)

VC Pool Size\*: 1000 (1 - 2147483646)

Save

Cancel

Note: \* - Required Field

111634

- Step 5    Enter an *VC Pool Start*. (50000).
- Step 6    Enter an *VC Pool Size*. (1000).
- Step 7    Click **Save**.

The **Resource Pools - VC ID** window appears, as shown in Figure 3-22.

Figure 3-22      Resource Pools - VC ID

Resource Pools

Pool Type: VCID

Refresh

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Start	Pool Size	Status
1.	<input type="checkbox"/>	50000	1000	Available

Rows per page: 10

Go to page: 1 of 1 Go

Create

Delete

111635

You have saved a VC ID Pool in the Repository.

# Create a VLAN Pool

This section describes how to create a VLAN (VC ID) Pool with the ISC GUI.

To create a VLAN Pool with the ISC GUI, follow these steps:

- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Resource Pools**.  
The **Resource Pools** window appears (not shown).
- Step 3** Choose **VLAN** from the **Pool Type** window.  
The **Resource Pools - VLAN** window appears, as shown in Figure 3-23.

**Figure 3-23 Resource Pools - VLAN**

- Step 4** Click **Create**.  
The **Create VLAN Pool** window appears, as shown in Figure 3-24.

**Figure 3-24 Choose Device**

- Step 5** Enter an *VLAN Pool Start*. (**500**)
- Step 6** Enter an *VLAN Pool Size*. (**100**)

**Step 7**    Click **Select**.

The Choose Access Domain window appears, as shown in Figure 3-25.

**Figure 3-25**    *Choose Access Domain*

111638

**Step 8**    Choose an **Access Domain**.

**Step 9**    Click **Select**.

The Create VLAN Pool window appears, as shown in Figure 3-26.

**Figure 3-26**    *Create VLAN Pool*

111639

**Step 10**    Click **Save**.

The Resource Pools - VLAN window appears, as shown in Figure 3-27.

**Figure 3-27 Resource Pools - VLAN**

**Resource Pools**

Pool Type:

Show VLAN Pools with Pool Name matching

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Start	Pool Size	Status	Pool Name
1.	<input type="checkbox"/>	500	100	Allocated	Provider-X:AD-North-X

Rows per page:

Go to page:  of 1

111640

You have saved a VLAN Pool in the Repository.





## Defining VPNs and CERCs

During service deployment, ISC generates the Cisco IOS commands to configure the logical VPN relationships.

At the beginning of the provisioning process, before creating a Service Policy, a VPN must be defined within ISC. The first element in a VPN definition is the name of the VPN.

This chapter describes how to define MPLS VPNs, IP Multicast VPNs, and CE Routing Communities (CERCs).

This chapter contains the following major sections:

- Creating MPLS VPN, page 4-1
- Creating IP Multicast VPN, page 4-3
- Creating CE Routing Communities, page 4-6

## Creating MPLS VPN

**Step 1** Log into ISC.

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

The VPN window appears, as shown in Figure 4-1.

**Figure 4-1** VPNs

**Step 3** Click **Create** to create a VPN.

The Create VPN window appears, as shown in Figure 4-2.

**Figure 4-2 Create VPN**

**Create VPN**

Name \*: west-xVPN

Customer \*: Cust-A Select

**MPLS Attributes**

Create Default CE Routing Community: ☐ Provider1 ▾

Enable Multicast: ☐

Enable Auto Pick MDT Addresses: ☒

Default MDT Address \*:  (a.b.c.d)

Data MDT Subnet:  (a.b.c.d)

Data MDT Size:  ▾

Data MDT Threshold:  (1 - 4294967 kilobits/sec)

Default PIM Mode: SPARSE\_DENSE\_MODE ▾

MDT MTU:  (576 - 18010)

Enable PIM SSM: ☐ DEFAULT ▾

SSM List Name \*:

Multicast Route Limit:  (1 - 2147483647)

Enable Auto RP Listener: ☐

Configure Static-RP: ☐

PIM Static-RPs \*: Showing 0 of 0 records Edit

#	Static-RP Unicast Address	Multicast-Group List Name	Override
Rows per page: 10 ▾ <span>Go to page: 1 of 1</span> <span>Go</span> <span>▹</span> <span>▹▹</span>			

CE Routing Communities:  Select Remove

158195

**Step 4** Enter the *VPN Name*. (**west-xVPN**)

**Step 5** For the Customer field, click **Select**.

The Choose Customer window appears, as shown in Figure 4-3.

**Figure 4-3 Choose Customer**

**Step 6** Choose a Customer and then click **Select**. (**Cust-A**)

The VPNs window reappears.

**Step 7** To associate the VPN with a Provider, you have two options:

- Go to **Create Default CE Routing Community**, then choose a **Provider**.
- Choose a CE Routing Community, if one is already set up.



**Note** To enable multicast for the VPN, see “Creating IP Multicast VPN”.

**Step 8** To save these changes, at the bottom of the window, click **Save**.

The VPN Name (**west-xVPN**) is associated with the Customer (**Cust-A**) in this new VPN definition.

## Creating IP Multicast VPN

**Step 1** To create an IP Multicast VPN, follow the procedure described in “Creating MPLS VPN” section on page 4-1 to the place where you can enable multicast for the VPN.

**Step 2** To enable multicast for the VPN, check **Enable Multicast**.

The current window will refresh with additional fields becoming active (see Figure 4-4).

**Figure 4-4** Creating Multicast VPN

**Create VPN**

Name \*: Jancar-MVPN

Customer \*: Customer2 Select

**MPLS Attributes**

Create Default CE Routing Community: ☒ Provider1

Enable Multicast: ☒

Enable Auto Pick MDT Addresses: ☐

Default MDT Address \*: 239.232.1.1 (a.b.c.d)

Data MDT Subnet: 239.232.2.0 (a.b.c.d)

Data MDT Size: 256

Data MDT Threshold: 50 (1 - 4294967 kilobits/sec)

Default PIM Mode: SPARSE\_MODE

MDT MTU: 1500 (576 - 18010)

Enable PIM SSM: ☒ RANGE

SSM List Name \*: ssmList

Multicast Route Limit: 10000 (1 - 2147483647)

Enable Auto RP Listener: ☒

Configure Static-RP: ☒

PIM Static-RPs \*: Showing 1 - 3 of 3 records Edit

#	Static-RP Unicast Address	Multicast-Group List Name	Override
1.	10.99.1.1	rpl1List	<input checked="" type="checkbox"/>
2.	10.99.1.2	rpl2List	<input type="checkbox"/>
3.	10.99.1.5		<input checked="" type="checkbox"/>

Rows per page: 10 Go to page: 1 of 1 Go

158190

- Step 3** For MDT (Multicast Distribution Tree) addresses, either accept the default (check box already checked) to enable the auto pick function, or uncheck the auto pick check box, then enter values in the next two fields:

Default MDT Address

Data MDT Subnet

- Step 4** From the drop-down list, choose a value for Data MDT Size.

- Step 5** In the next field, enter a valid value for Data MDT Threshold (1 - 4294967 kilobits/sec).

- Step 6** For Default PIM (Protocol Independent Multicast) Mode, choose a mode from the drop-down list:

SPARSE\_MODE

SPARSE\_DENSE\_MODE

**Tip**

Multicast routing architecture allows the addition of IP multicast routing on existing IP networks. PIM is an independent unicast routing protocol. It can be operated in two modes: dense and sparse.

- Step 7** In the next field, enter a valid value for MDT MTU (Maximum Transmission Unit).
- Step 8** To enable PIM SSM (Source Specific Multicast), check the associated check box.
- When you check the check box:
- The associated drop-down list goes active with the DEFAULT enumeration populated as the SSM default. This will create the following CLI: **ip pim vrf <vrfName> ssm default**.
  - If you would like to associate an access-list number, or a named access-list, with SSM configuration, choose the RANGE enumeration from the SSM drop-down list instead of DEFAULT. This will create the following CLI: **ip pim vrf <vrfName> ssm range {ACL# | named-ACL-name}**.
- Step 9** If you choose RANGE in the previous step, then the next field goes active for you to enter Access-list number or Access-list name.
- Step 10** In the next field enter a valid value for the Multicast Route Limit (1 - 2147483647).
- Step 11** To enable the auto RP (Rendezvous Point) listener function, check the associated check box.
- Step 12** To configure Static-RPs, check the associated check box.
- When you check this, the Edit option for PIM Static-RPs goes active.
- Step 13** To edit, or add, PIM Static RPs (Rendezvous Points), click **Edit**.
- The Edit PIM Static RPs window appears, see Figure 4-5).

**Figure 4-5** Edit PIM Static RPs

#	<input type="checkbox"/>	Static-RP Unicast Address	Multicast-Group List Name	Override
1.	<input type="checkbox"/>	10.99.1.1	rp1List	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	10.99.1.2	rp12List	<input type="checkbox"/>
3.	<input type="checkbox"/>	10.99.1.5		<input checked="" type="checkbox"/>

Showing 1 - 3 of 3 records

Rows per page: 10 Go to page: 1 of 1 Go

Add Delete OK Cancel

- Step 14** Complete all applicable fields in the Edit PIM Static RP window, then click **OK**.
- These data now appear in the main Create VPN window (see Figure 4-4).
- Step 15** To save your changes and add this Multicast VPN to you system, at the bottom of the window, click **Save**.

# Creating CE Routing Communities

When you create a VPN, the ISC software creates one default CE routing community (CERC) for you. But if your network topology and configuration require customized CERC definitions, you can define CERCs customized for your network.



**Tip**

Customized CERCs should be defined only in consultation with the VPN network administrator.

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

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

To define a new CERC:

**Step 1** Click the **Service Inventory** tab.

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

The Inventory and Connection Manager window appears.

**Step 3** Go to **CE Routing Communities**.

The CE Routing Communities dialog box appears (see Figure 4-6).

**Figure 4-6** CE Routing Communities Defined for This VPN

#	Name	HRT	SRT	Provider	VPN
1.	Default	99:0	99:1	FirstProvider	AcmeIncVPN
2.	Default	99:2	99:3	FirstProvider	WidgetsIncVPN
3.	Default	99:4	99:5	FirstProvider	

Rows per page: 10

Create Edit Delete

**Step 4** From the CE Routing Communities dialog box, click **Create**.

The Create CE Routing Community dialog box appears (see Figure 4-7).

**Figure 4-7** Defining a New CE Routing Community

**Step 5** Complete the CERC fields as required for the VPN:

- c. *Provider:* To specify the service provider associated with this CERC, click **Select**.

The Choose Provider dialog box appears.

- d. Choose the name of the service provider, then click **Select**.

- e. *Name:* Enter the name of the CERC.

- f. *CERC Type:* Specify the CERC type: *Hub and Spoke* or *Fully Meshed*.

- g. *Auto-Pick Route Target Values:* Choose to either let ISC automatically set the route target (RT) values or set the RT values manually.

By default, the **Auto-pick route target values** check box is checked. If you uncheck the check box, you can enter the Route Target values manually.



**Caution**

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

**Step 6** When you have finished entering the information in the Create CE Routing Community dialog box, click **Save**.





# MPLS VPN Service Policies

---

This chapter describes how to use the IP Solution Center (ISC) GUI to define MPLS VPN Service Policies. This chapter contains the following major sections:

- Service Policy Overview, page 5-1
- Creating Service Policies, page 5-6
- Creating MPLS Service Policy for PE-to-CE Link, page 5-7
- Defining an MVRFCE PE-CE Service Policy, page 5-34

## Service Policy Overview

Provisioning an MPLS VPN begins with defining a service policy. A service policy can be applied to multiple PE-CE links in a single service request.

A *network operator* defines service policies. A *service operator* uses a service policy to create service requests. Each service request contains a list of PE-CE links. When a service operator creates a service request, the operator sees only the policy information required to be completed. All the other necessary information is filled in by the service policy itself (as well as the Auto Discovery process).

## Creating MPLS VPN in ISC

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

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

To create a new VPN in ISC: MPLS, follow these steps:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Log in to ISC.                          |
| <b>Step 2</b> | Click the <b>Service Inventory</b> tab. |

**Step 3** Go to **Inventory and Connection Manager**.

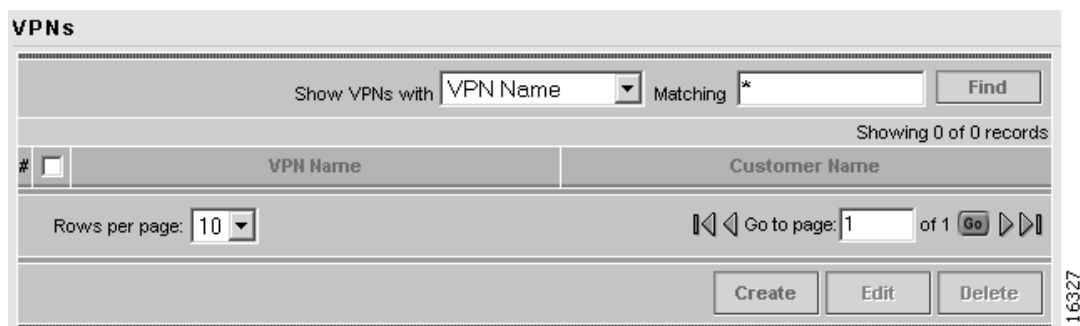
The Inventory and Connection Manager window appears (see Figure 5-1).

**Figure 5-1** *Creating an MPLS VPN in ISC*

**Step 4** From the Inventory and Connection Manager, choose **VPNs**.

The VPNs dialog box appears (see Figure 5-2).

**Figure 5-2** *Viewing Existing VPNs or Creating a New VPN*

**Step 5** From the VPNs dialog box, click **Create**.

The Create VPN dialog box appears (see Figure 5-3).

**Figure 5-3** Creating an MPLS VPN in ISC

**Create VPN**

Name \*:

Customer \*:

**MPLS Attributes**

Create Default CE Routing Community: ☒

Enable Multicast: ☐

Data MDT Size:

Data MDT Threshold:  (1 - 4294967 bits/sec)

CE Routing Communities:

**VPLS Attributes**

Enable VPLS: ☐

Service Type:

Topology:

Note: \* - Required Field

**Step 6** *Name:* Enter the name of the VPN:

**Step 7** *Customer:* To choose the customer associated with this VPN:

- a. Click **Select**.

The Select Customer dialog box appears (see Figure 5-4).

**Figure 5-4** Selecting a Customer for the VPN

**Select Customer - Microsoft Internet Explorer**

Show Customers with Customer Name matching \*

Showing 1 - 3 of 3 records

#	Customer Name	Customer Name
1.	<input checked="" type="radio"/> CUST1	
2.	<input type="radio"/> Customer_Ford	
3.	<input type="radio"/> DiscoveredL2Customer	

Rows per page:

- b. From the list of customers, choose the appropriate customer, then click **Select**.

**Step 8** *Create Default CE Routing Community:* To create a default CE routing community, choose the **Create Default CE Routing Community** check box and choose a provider.

**Step 9** *Enable Multicast:*

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

**Note**

Before you can create a VPN with multicast enabled, you must define one or more multicast resource pools. See *Create a Multicast Pool*, page 3-4, for further information.

- a. To enable multicast VPN routing, check the **Enable Multicast** check box.

ISC enables two additional fields required to configure multicast routing (see Figure 5-5).

**Figure 5-5**      **Selecting a Customer for the VPN**

To implement multicast routing, ISC employs the concept of a *multicast domain* (MD), which is a set of VRFs associated with interfaces that can send multicast traffic to each other. A VRF contains VPN routing and forwarding information for unicast. A *multicast VRF* contains multicast routing and forwarding information and supports multicast routing.

- b. *Data MDT Size*: From the drop-down list, choose the data MDT size.

MDT refers to a *multicast distribution tree* (MDT). The MDT defined here carries multicast traffic from customer sites associated with the multicast domain.

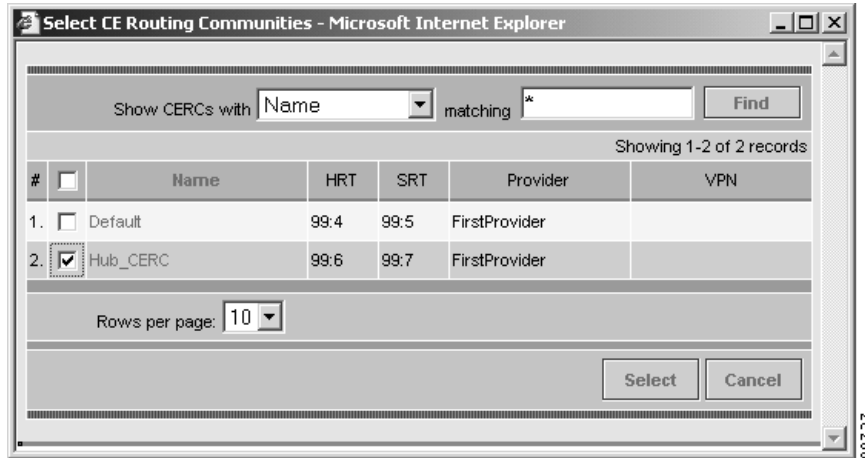
- c. *Data MDT Threshold*: Enter the bandwidth threshold for the data multicast distribution tree.

The *data MDT* contains a range of multicast group addresses and a bandwidth threshold. Thus, whenever a CE behind a multicast-VRF exceeds that bandwidth threshold while sending multicast traffic, the PE sets up a new data MDT for the multicast traffic from that source. The PE informs the other PEs about this data MDT and, if they have receivers for the corresponding group, the other PEs join this data MDT.

**Step 10** *CE Routing Communities*: If you do not choose to enable the default CERC, you can choose a customized CERC that you have already created in ISC (see *Creating CE Routing Communities*, page 4-6):

- a. From the CE Routing Communities pane, click **Select**.

The Select CE Routing Communities dialog box appears (see Figure 5-6).

**Figure 5-6**      **Selecting a CERC**

- b. Click the check box for the CERC you want used for this VPN, then click **Select**.

You return to the Create VPN dialog box, where the new CERC selection appears, along with its *hub route target (HRT)* and spoke route target (SRT) values (see Figure 5-7).

**Figure 5-7**      **New CERC Selected**

**MPLS Attributes**

Create Default CE Routing Community: ☒ PROV1

Enable Multicast: ☒

Data MDT Size: 16

Data MDT Threshold: 0 (1 - 4294967 bits/sec)

CE Routing Communities: CERC2: 100:604(HRT)/100:605(SRT)

**VPLS Attributes**

Enable VPLS: ☐

Service Type: ERS

Topology: Full Mesh

- Step 11** **Enable VPLS** (optional) check this check box to enable VPLS.
- Step 12** **Service Type** (optional) choose the VPLS service type from the drop-down menu: **ERS** (Ethernet Relay Service) or **EWS** (Ethernet Wire Service).
- Step 13** **Topology** (optional) choose the VPLS topology from the drop-down menu: **Full Mesh** (each CE will have direct connections to every other CE) or **Hub and Spoke** (only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other).
- Step 14** When satisfied with the settings for this VPN, click **Save**.

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

# Creating Service Policies

Provisioning an MPLS VPN begins with defining a service policy. A service policy can be applied to multiple PE-CE links in a single service request.

A *network operator* defines service policies. A *service operator* uses a service policy to create service requests. Each service request contains a list of PE-CE links. When a service operator creates a service request, the operator sees only the policy information required to be completed. All the other necessary information is filled in by the service policy itself (as well as the Auto Discovery process).

## Service Policy Editor

When you define a service policy for ISC, you are presented with a series of dialog boxes that allow you to specify the parameters for each major category required to complete an MPLS service request. The Service Policy editor presents three columns: **Attribute**, **Value**, and **Editable**:

- **Attribute**

The *Attribute* column displays the names of each parameter that you need to define for each major category (for example, IP addresses or routing protocols).

- **Value**

The *Value* column displays the fields and other selectable items that correspond to each parameter and option.

The type of dialog box that is invoked when you edit an attribute depends on the type of attribute. In some cases, the value is a simple string value or integer value, in which case a single text entry field appears. In other cases, the value is complex or consists of multiple values, such as an IP address. In these cases, a dialog box appears so you can specify the required values. The values you enter are validated; when invalid values are entered, you receive notification of the invalid values. In other cases, you will be presented with check boxes that will allow you to enable or disable a particular option.

**Note**

In some cases, changing an attribute's value results in invalidating the values of related attributes. For example, changing the PE interface name can result in invalidating the PE encapsulation value. When this occurs, the service policy editor removes the invalid values and you will need to reset them appropriately.

There is a parent-child relationship between some attributes. In these cases, changing the value of a parent attribute can enable or disable the child attributes. For example, changing the value of the PE encapsulation could result in enabling or disabling the DLCI (data link connection identifier), VLAN ID, ATM circuit identifiers, and the tunnel source and destination address attributes.

- **Editable**

The Editable column allows the network operator to indicate the attributes that are likely to change across multiple service requests. When attributes are checked as editable, only those attributes will be made available to the service operator when creating or modifying service requests with that service request policy.

When an attribute category is set to be editable, all the related and child attributes are also editable attributes.

## About IP Addresses in Cisco ISC

Within a VPN (or extranet), all IP addresses must be unique. Customer IP addresses are not allowed to overlap with provider IP addresses. Overlap is possible only when two devices cannot see each other; that is, when they are in isolated, non-extranet VPNs.

The ISC: MPLS software assumes that it has an IP address pool to draw addresses from. The only way to guarantee that the product can use these addresses freely is if they are provider IP addresses.

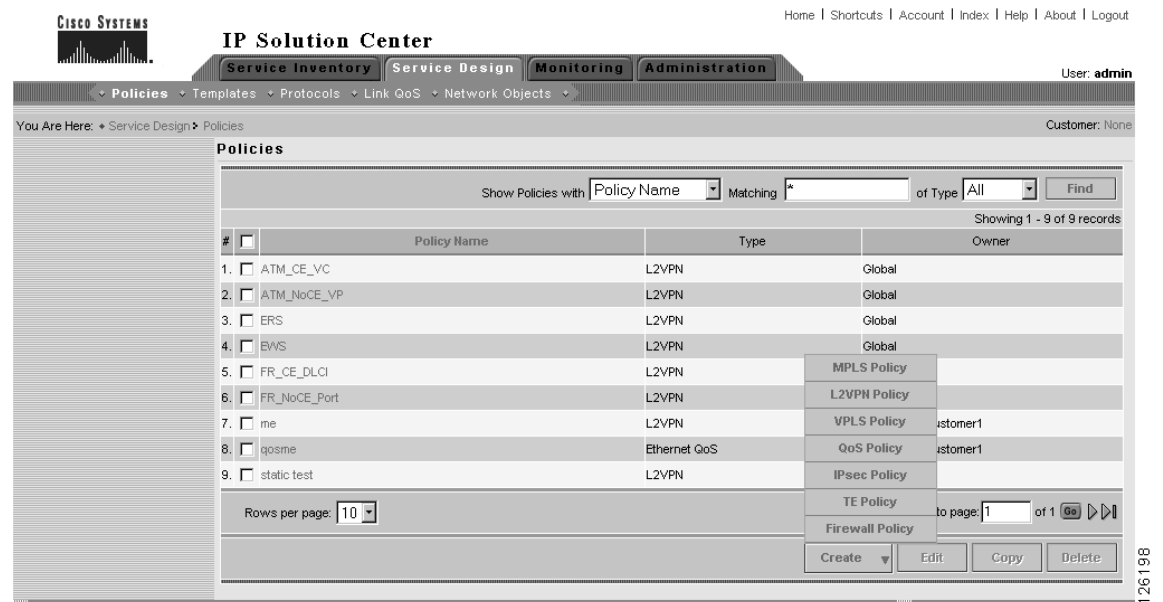
Predefining a unique section (or sections) of IP address space for the PE-CE links is the only way to ensure stable security. Thus, because of the security and maintenance issues, Cisco does not recommend using customer IP addresses on the PE-CE link.

## Creating MPLS Service Policy for PE-to-CE Link

To create an MPLS service policy for a PE-to-CE link, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Click the **Service Design** tab.
- Step 3** Go to **Policies**.  
The Policies window appears (see Figure 5-8).

**Figure 5-8** Creating a New Service Policy



- Step 4** From the **Create** drop-down list, choose **MPLS Policy**.  
The MPLS Policy Type dialog box appears (see Figure 5-9).

**Figure 5-9** Defining the MPLS Service Policy

You Are Here: +

Mode: ADDING

1. Step 1: Policy Type

2. ...

MPLS Policy Editor - Policy Type

Attribute	Value
Policy Name *	mpls_pe_ce
Policy Owner *	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
Customer *	Select
Policy Type *	<input checked="" type="radio"/> Regular: PE-CE <input type="radio"/> MVRFCPE: PE-CE
CE Present *	<input checked="" type="checkbox"/>

89742

**Step 1** Enter a **Policy Name** for the MPLS policy.

**Step 2** Choose the **Policy Owner**.

There are three types of MPLS policy ownership:

- Customer ownership
- Provider ownership
- Global ownership: Any service operator can make use of this MPLS policy.

This ownership has relevance when the ISC Role-Based Access Control (RBAC) comes into play. For example, an MPLS 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 3** Click **Select** to choose the owner of the MPLS 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 4** Choose the **Policy Type** of the MPLS policy.

There are two policy types for MPLS policies:

- Regular PE-CE: PE-to-CE link
- MVRFCPE PE-CE: PE to CE link using the Multi-VRF feature for the PE

**Step 5** Choose the **CE Present** check box if you want ISC to ask the service operator who uses this MPLS policy to provide a CE router and interface during service activation. The default is CE present in the service.

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

**Step 6** Click **Next**.

## Specifying PE and CE Interface Parameters

The MPLS Policy Interface dialog box appears (see Figure 5-10).

**Tip**

You do not have to choose a specific interface type for the PE and CE at this point. Notice that the fields are set by default to **Editable**. With the interface parameters set to **Editable**, the service operator can specify the exact interface type and format when he or she creates the service request.

If you want to specify the device interface information for this service policy when the service request is created, leave the fields as they are currently set by default, then click **Next**.

**Figure 5-10** Specifying the PE UNI Security, and CE Interface Parameters

**MPLS Policy Editor - Interface**

Attribute	Value	Editable
<b>Reset All Attribute Editable Flags:</b>		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY <input type="button" value="v"/>	
Interface Format:	<input type="text"/>	
Interface Description:	<input type="text"/>	<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Auto-Pick VLAN ID:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use SVI:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Link Speed:	None <input type="button" value="v"/>	<input checked="" type="checkbox"/>
Link Duplex:	None <input type="button" value="v"/>	<input checked="" type="checkbox"/>
ETTH Support:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Standard UNI Port:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Security Information</b>		
Disable CDP:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Filter BPDU:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use Existing ACL Name:	<input type="checkbox"/>	
UNI MAC Addresses:	<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>
UNI Port Security:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Maximum MAC Address:	<input type="text"/> (1 - 5120)	<input checked="" type="checkbox"/>
Aging (in minutes):	<input type="text"/> (0 - 1440)	<input checked="" type="checkbox"/>
Violation Action:	PROTECT <input type="button" value="v"/>	<input checked="" type="checkbox"/>
Secure MAC Addresses:	<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>
<b>CE Information</b>		
Interface Type:	ANY <input type="button" value="v"/>	
Interface Format:	<input type="text"/>	
Interface Description:	<input type="text"/>	<input checked="" type="checkbox"/>

138950

To specify the PE, UNI Security, and CE interface information for this MPLS policy:

#### PE Interface Information

**Step 1** *Interface Type:* From the drop-down list, choose the interface type for the PE.

IP Solution Center supports the following interface types (for both PEs and CEs):

- Any
- ATM (Asynchronous Transfer Mode)
- BRI (Basic Rate Interface)
- Ethernet
- Fast Ethernet
- FDDI (Fiber Distributed Data Interface)
- GE-WAN (Gigabit Ethernet WAN)
- Gigabit Ethernet
- HSSI (High Speed Serial Interface)
- Loopback
- MFR
- MultiLink
- PoS (Packet over Sonet)
- Port-Channel
- Serial
- Switch
- Tunnel
- VLAN

**Step 2** *Interface Format:* Optionally, you can specify the slot number and port number for the PE interface.

Specify the format in the standard nomenclature: **slot number/port number** (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. If this parameter is left editable, it can be changed when the service operator creates the service request.

You can also specify the Interface Format as a Channelized Interface:

- **slot/subSlot/port** (for example, **2/3/4** indicates that the interface is located at Serial 2/3/4)
- **slot/subSlot/port/T1#:channelGroup#** (for example, **2/0/4/6:8** indicates that the interface is located at Serial 2/0/4/6:8)
- **slot/subSlot/port.STS-1Path/T1#:channelGroup#** (for example, **2/0/0.1/6:8** indicates that the interface is located at Serial 2/0/0.1/6:8)

**Step 3** *Interface Description:* Optionally, you can enter a description of the PE interface.

**Step 4** *Shutdown Interface:* When you enable this check box, the specified PE interface is configured in a shut down state.

**Step 5** *Encapsulation:* Choose the encapsulation used for the specified PE interface type.

When you choose an interface type, the *Encapsulation* field displays a drop-down list of the supported encapsulation types for the specified interface type.

Table 5-1 shows the protocol encapsulations available for each of the supported interface types.

**Table 5-1**      **Interface Types and Their Corresponding Encapsulations**

Interface Type	Encapsulations
ATM	AAL5SNAP
BRI	Frame-Relay, Frame-Relay-ietf, HDLC (High-Level Data Link Control), PPP (Point-to-Point Protocol).  <b>Frame-Relay-ietf</b> sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this method when connecting to another vendor's equipment across a Frame Relay network.
Ethernet	Default frame, Dot1Q (802.1Q)
Fast Ethernet	Default frame, ISL (Inter-Switch Link), Dot1Q (802.1Q)
FDDI (Fiber Distributed Data Interface)	None
Gigabit Ethernet	Default frame, ISL (Inter-Switch Link), Dot1Q (802.1Q)
Gigabit Ethernet WAN	Default frame, ISL (Inter-Switch Link), Dot1Q (802.1Q)
HSSI (High Speed Serial Interface)	Frame-Relay, Frame-Relay-ietf, HDLC (High-Level Data Link Control), PPP (Point-to-Point Protocol)
Loopback	None.
MFR	Frame-Relay, Frame-Relay-ietf, HDLC (High-Level Data Link Control), PPP (Point-to-Point Protocol).
MultiLink	PPP (Point-to-Point Protocol)
Port-Channel	Default frame, ISL (Inter-Switch Link), Dot1Q (802.1Q)
POS (Packet Over Sonet)	Frame-Relay, HDLC (High-Level Data Link Control), PPP (Point-to-Point Protocol)
Serial	Frame-Relay, Frame-Relay-ietf, HDLC (High-Level Data Link Control), PPP (Point-to-Point Protocol)
Switch	AAL5SNAP
Tunnel	GRE (Generic Routing Encapsulation) - <b>GRE is not supported in this release.</b> -
VLAN	None

**Step 6**    *Auto-Pick VLAN ID:* Enable this check box to have ISC automatically pick the VLAN ID.

**Step 7**    *Use SVI:* Enable this check box to have ISC terminate VRF on SVI.

**Step 8**    *Link Speed:* Enter a Link Speed (optional) of 10, 100, 1000, or auto.

**Step 9**    *Link Duplex:* Enter a Line Duplex (optional) of full, half, or auto.

**Step 10**   *ETTH Support:* Enable this check box to configure Ethernet-To-The-Home (ETTH). See Ethernet-To-The-Home, page 12-9 for an explanation of ETTH.

**Step 11**   *Standard UNI Port:* Enable this check box to access UNI Security Parameters:

#### UNI Security Information

**Step 12**   *Disable CDP:* Enable this check box to disable CDP.

**Step 13**   *Filter BPDU:* Enable this check box to filter BPDU.

- Step 14** *Use existing ACL Name:* Enable this check box to use existing ACL name.
- Step 15** *UNI MAC Addresses:* Click **Edit** to modify or create a MAC address record.
- Step 16** *UNI Port Security:* Enable this check box to access UNI Port Security parameters:
- Maximum MAC Address:* Enter a valid value.
  - Aging (in minutes):* Enter a valid value.
  - Violation Action:* From the drop-down list, choose one of the following:  
PROTECT  
RESTRICT  
SHUTDOWN
  - Secure MAC Address:* Click **Edit** to modify or create a secure MAC address record.

#### CE Interface Information

- Step 17** *Interface Type:* From the drop-down list, choose the interface type for the CE.
- Step 18** *Interface Format:* Optionally, you can specify the slot number and port number for the CE interface.
- Step 19** *Interface Description:* Optionally, you can enter a description of the CE interface.
- Step 20** *Encapsulation:* Choose the encapsulation used for the specified CE interface type.
- Step 21** When satisfied with the interface settings, click **Next**.

## Specifying IP Address Scheme

The MPLS Policy Interface Address Selection dialog box appears (see Figure 5-11). This lets you specify the IP address scheme you want to use for this service policy.

**Figure 5-11** Specifying the IP Address Scheme

Attribute	Value	Editable
<b>PE-CE Interface Addresses/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Extra CE Loopback Required:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

- Step 1** Define the IP addressing scheme that is appropriate for the PE-CE link.

#### IP Numbering Scheme

A point-to-point link between two routers can be either a *numbered* IP address or an *unnumbered* IP address. The service provider must determine whether to use numbered or unnumbered IP addresses for the PE-CE link. Defining the link to use unnumbered addresses can save precious IP addresses because many interfaces can borrow the same IP address.

You can choose among two options: **IP Numbered** or **IP Unnumbered**.

- **IP Numbered**

If you choose **IP numbered** and choose to not use automatically assigned IP addresses, you can enter the IP addresses for the PE interface and CE interface in the fields provided. Entering the IP addresses in these fields forces the MPLS VPN software to use the indicated addresses.

If you choose **IP numbered** and also enable the **Automatically Assign IP Address** check box, ISC: MPLS checks for the presence of the corresponding IP addresses in the router's configuration file. If the addresses are present and they are in the same subnet, ISC uses those addresses (and does not allocate them from the address pool). If the IP addresses are not present in the configuration file, ISC picks IP addresses from a /30 subnet point-to-point IP address pool.

- **IP Unnumbered**

IP addresses are drawn from the loopback IP address pool. An unnumbered IP address means that each interface "borrows" its address from another interface on the router (usually the loopback interface). Unnumbered addresses can only be used on point-to-point WAN links (such as Serial, Frame, and ATM), not on LAN links (such as Ethernet). If using IP unnumbered, then both the PE and CE must use the same IP unnumbered addressing scheme. When you choose **IP unnumbered**, ISC: MPLS creates a static route for the PE-CE link.

When you choose **IP unnumbered**, ISC: MPLS automatically creates a loopback interface (unless a loopback interface already exists with the correct attributes). For related information, see Using Existing Loopback Interface Number, page 5-14.

If you choose **IP unnumbered** and choose to not use automatically assigned IP addresses, you can enter the IP addresses for the PE interface and CE interface in the fields provided. Entering the IP addresses in these fields forces the ISC: MPLS software to use the indicated addresses.

**Step 2** Indicate whether an extra loopback interface is required for the CE.

**Extra CE Loopback Required**

Even though a numbered IP address does not require a loopback address, ISC software provides the option to specify that an extra CE loopback interface is required. This option places an IP address on a CE router that is not tied to any physical interface.

If you enable **Extra CE Loopback Required**, you can enter the CE loopback address.

**Step 3** Specify whether you want to automatically assign IP addresses.

**Automatically Assign IP Address**

If you choose **IP unnumbered** and also enable the **Automatically Assign IP Address** check box, ISC picks two IP addresses from a /32 subnet point-to-point IP address pool.

If you choose **IP numbered** and also enable the **Automatically Assign IP Address** check box, ISC checks for the presence of the corresponding IP addresses in the router's configuration file. If the addresses are present and they are in the same subnet, ISC uses those addresses (and does not allocate them from the address pool). If the IP addresses are not present in the configuration file, ISC picks IP addresses from a /30 subnet point-to-point IP address pool.

**Step 4** Specify the IP address pool and its associated Region for this service policy.

**IP Address Pool**

The IP Address Pool option gives the service operator the ability to have ISC automatically allocate IP addresses from the IP address pool attached to the Region. Prior to defining this aspect of the service policy, the Region must be defined and the appropriate IP address pools assigned to the Region.

You can specify IP address pool information for *point-to-point (IP numbered)* PE-CE links.

IP unnumbered addresses are drawn from the loopback IP address pool. An unnumbered IP address means that each interface “borrows” its address from another interface on the router (usually the loopback interface). Unnumbered addresses can only be used on point-to-point WAN links (such as Serial, Frame, and ATM), not on LAN links (such as Ethernet). If using IP unnumbered, then both the PE and CE must use the same IP unnumbered addressing scheme.

**Step 5** When satisfied with the IP address scheme, click **Next**.

## Using Existing Loopback Interface Number

On each PE, there is usually only one loopback interface number per VRF for interfaces using IP unnumbered addresses. However, if provisioning an interface using IP unnumbered addresses and manually assigned IP addresses, it is possible to have more than one loopback interface number under the same VRF. When using automatically-assigned IP addresses for provisioning IP unnumbered addresses, ISC associates the first loopback number with the same VRF name to the interface. If no loopback number already exists, ISC creates one.

If a service provider wants ISC to use an existing loopback interface number (for example, Loopback0), the service provider must modify the loopback interface description line in the configuration files for the pertinent routers (PE or CE).

To use the existing loopback interface number, you must modify the loopback interface description line so that it includes the keyword **VPN-SC**, as shown in the following example of a router configuration file.



### Note

When using an existing loopback interface number on a PE, an additional command line with the “ip vrf forwarding <VRF\_name>” command must be included directly after the “description” line.

```
interface Loopback0
description by VPN-SC
ip vrf forwarding <VRF_name> ; This line is required on the PE only
ip address 209.165.202.129 255.255.255.224
```

You can use an existing loopback interface number only when the interface configuration meets these conditions: it must be a WAN serial interface using IP unnumbered addresses.

ISC selects loopback interface numbers by sequence. ISC uses the first loopback interface number that meets the requirement—for a CE, it is inclusion of the VPN-SC keyword; for a PE, it is the matching VRF name.

For example, if loopback1 and loopback2 include the VPN-SC keyword, but loopback3 does not, adding the VPN-SC keyword to loopback3 will not force ISC to choose loopback3 for the unnumbered interface when using automatically assigned addresses. Loopback1 will be chosen instead. The only way to choose a specific loopback interface number is to use a manually assigned IP address that matches the desired loopback interface number.



### Note

Unlike standard interfaces, when loopback interfaces are provisioned in ISC, the resulting configuration file does not include a Service Request (SR) ID number. This is because multiple interfaces or service requests can use the same loopback interface.

## Specifying Routing Protocol for a Service

You can now specify the routing protocol information for this service policy (see Figure 5-12).

The routing protocol you choose must run on both the PE and the CE. You can choose any one of the following protocols:

- **Static.** Specifies a static route (see Static Protocol Chosen, page 5-16).
- **RIP.** Routing Information Protocol (see RIP Protocol Chosen, page 5-17).
- **BGP.** Border Gateway Protocol (see BGP Protocol Chosen, page 5-21).
- **OSPF.** Open Shortest Path First (see OSPF Protocol Chosen, page 5-24).
- **EIGRP.** Enhanced Interior Gateway Routing Protocol (see EIGRP Protocol Chosen, page 5-28).
- **None.** *Specifies parameters for cable services (see None Chosen: Cable Services, page 5-33).*

To specify a routing protocol for the PE-CE link:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Choose the appropriate protocol from the Routing Protocol drop-down list.<br><br>When you choose a particular routing protocol, the related parameters for that protocol are displayed. |
| <b>Step 2</b> | Enter the required information for the selected routing protocol, then click <b>Next</b> .  |
| <b>Step 3</b> | Define the MPLS Policy VRF and VPN Selection parameters as described in Defining the Service Policy VRF and VPN Information, page 5-39.   |
- 

## Redistribution of IP Routes

*Route redistribution* is the process of taking routing information from one source and importing that information into another source. Redistribution should be approached with caution. When you perform route redistribution, you lose information. Metrics must be arbitrarily reset. For example, if a group of RIP routes with a metric of five hops is redistributed into IGRP, there is no way to translate the five hop RIP metric into the composite metric of IGRP. You must arbitrarily choose a metric for the RIP routes as they are redistributed into IGRP. Also, when redistribution is performed at two or more points between two dynamic routing protocol domains, routing loops can occur.

## CSC Support

To define a Service Policy with Carrier Supporting Carrier (CSC), choose the CSC Support check box from the MPLS Policy Editor - Routing Information. When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service. Provisioning CSC is explained in Chapter 11, “Provisioning Carrier Supporting Carrier.”

## Giving Only Default Routes to CE

When you enable the **Give only default routes to CE** option, you indicate whether the site needs *full routing* or *default routing*. Full routing is when the site must know specifically which other routes are present in the VPN. Default routing is when it is sufficient to send all packets that are not specifically for your site to the VPN.

If you choose this option, ISC configures the **default-info originate** command on the PE router under the running protocol (for RIP, OSPF, or EIGRP). For Static, ISC configures an **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** command on the CE router.

A device can only have one default route. Therefore, the VPN can use a default route, but only on condition that the customer site does not already have a different one. The most common reason to already have a default route is that the site has an Internet feed that is independent of the VPN.

If the CE site already has Internet service, the CE can either route all packets to unknown destinations to the Internet or learn all the routes in the Internet. The obvious choice is to route all packets to unknown destinations to the Internet. If a site has an Internet feed, it may already have a default route. Under such conditions, setting the VPN as the default route is incorrect; the VPN should only route packets meant for other VPN sites.

## Static Protocol Chosen

Static routing refers to routes to destinations that are listed manually in the router. Network reachability in this case is not dependent on the existence and state of the network itself. Whether a destination is up or down, the static routes remain in the routing table and traffic is still sent to that destination.

When you choose **Static** as the protocol, four options are enabled: **CSC Support**, **Give Only Default Routes to CE**, **Redistribute Connected (BGP only)**, and **Default Information Originate (BGP only)** (see Figure 5-12).



### Note

Two other options (**AdvertisedRoutes** and **Default Routes - Routes to reach other sites**) are available when you create the service request. See Static Routing Protocols, page 6-14.

**Figure 5-12** Specifying the Static Routing Protocol

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	STATIC	<input checked="" type="checkbox"/>
CsC Support:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Step 1** *CSC Support:* To define a Service Policy with Carrier Supporting Carrier (CSC), choose the CSC Support check box from the MPLS Policy Editor - Routing Information. When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service. Provisioning CSC is explained in Chapter 11, “Provisioning Carrier Supporting Carrier.”

**Step 2** *Give Only Default Routes to CE:* Specify whether this service policy should give only default routes to the CE when provisioning with static routes.

When you enable the **Give only default routes to CE** option with static route provisioning on the PE-CE link, ISC creates a default route on the CE that points to the PE. The VRF static route to the CE site is redistributed into BGP to other sites in the VPN.

When you choose this option, the default route (0.0.0.0/32) is automatically configured; the site contains no Internet feed or any other requirement for a default route. When the site encounters a packet that does not route locally, it can send the packet to the VPN.

If you choose this option, ISC configures **the default-info originate** command on the PE router under the running protocol (for RIP, OSPF, or EIGRP). For Static, ISC configures an **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** command on the CE router.

- Step 3** *Redistribute Connected (BGP Only)*: Indicate whether this service policy should redistribute the connected routes to the other CEs in the VPN.

When you enable the **Redistribute Connected** option, the connected routes (that is, the routes to the directly connected PEs or CEs) are distributed to all the other CEs in that particular VPN. This option is meant for IBGP if the routing protocol between PE-CE is a non-BGP protocol. For example, if the routing protocol is RIP, OSPF, EIGRP, or Static, the option is meant for the router bgp that is configured on the PE for the MPLS core. On the PE router, there is one router bgp process running at all times for MPLS. This option is also for BGP.



**Tip**

You must enable the **Redistribute Connected** option when joining the management VPN and you are also using IP numbered addresses.

- Step 4** *Default Information Originate (BGP only)*: When you enable this option, ISC issues a **default-information-originate** command under the iBGP address family for the currently specified VRF.

The **Default Information Originate** option is required, especially in the hub and spoke topology because each spoke must be able to communicate with every other spoke (by injecting a default route in the hub PE to the spoke PEs).

- Step 5** When finished defining static routing for this service policy, click **Next**.

The MPLS Policy VRF and VPN Membership dialog box appears. To proceed, see Defining the Service Policy VRF and VPN Information, page 5-39.

## RIP Protocol Chosen

The Routing Information Protocol (RIP) is a distance-vector protocol that uses hop count as its metric. RIP is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system. RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by one, and the sender is specified as the next hop.

RIP routers maintain only the best route to a destination—that is, the route with the lowest possible metric value. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers transmit.

- Step 1** To specify RIP as the routing protocol for the service policy, choose **RIP** from the Routing Protocol drop-down list.

The RIP Routing Protocol dialog box appears (see Figure 5-13).

**Figure 5-13** *RIP Selected as the Routing Protocol*

You Are Here: + Service Design > Policies Customer: None

MPLS Policy Editor - Routing Information

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	RIP	<input checked="" type="checkbox"/>
CsC Support:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RIP Metrics (BGP only):	(1-16)	<input checked="" type="checkbox"/>
Redistributed Protocols on PE:	Edit	<input checked="" type="checkbox"/>
Redistributed Protocols on CE:	Edit	<input checked="" type="checkbox"/>

Mode: ADDING

- ☒ 1. Policy Type
- ☒ 2. PE-CE Interface
- ☒ 3. PE-CE IP Address Scheme
- ☐ 4. PE-CE Routing Information
- ☐ 5. VRF and VPN Membership

126200

**Step 2** *CSC Support:* To define a Service Policy with Carrier Supporting Carrier (CSC), choose the CSC Support check box from the MPLS Policy Editor - Routing Information. When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service. Provisioning CSC is explained in Chapter 11, “Provisioning Carrier Supporting Carrier.”

**Step 3** *Give Only Default Routes to CE:* Specify whether you want to give only the default routes to the CE.

When an internetwork is designed hierarchically, *default routes* are a useful tool to limit the need to propagate routing information. Access-level networks, such as branch offices, typically have only one connection to headquarters. Instead of advertising all of an organization’s network prefixes to a branch office, configure a default route. If a destination prefix is not in a branch office’s routing table, forward the packet over the default route. The Cisco IP routing table displays the default route at the top of the routing table as the “Gateway of Last Resort.” RIP automatically redistributes the 0.0.0.0 0.0.0.0 route.

If you choose this option, ISC configures the **default-info originate** command on the PE router under the running protocol (for RIP, OSPF, or EIGRP). For Static, ISC configures an **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** command on the CE router.

When you enable the **Give Only Default Routes to CE** option for RIP, ISC creates a default RIP route on the PE; the default RIP route points to the PE and is sent to the CE. The provisioning request gives you the option of redistributing any other routing protocols in the customer network into the CE RIP routing protocol. The RIP routes on the PE to the CE site are redistributed into BGP to other VPN sites.

When you choose this option for RIP routing, the PE instructs the CE to send any traffic it cannot route any other way to the PE. Do *not* use this option if the CE site needs a default route for any reason, such as having a separate Internet feed.

**Step 4** *Redistribute Static (BGP and RIP):* Specify whether you want to redistribute static routes into the core BGP network.

When you enable the **Redistribute Static** option for RIP, the software imports the static routes into the core network (running BGP) and to the CE (running RIP).

**Step 5** *Redistribute Connected (BGP Only):* Specify whether you want to redistribute the connected routes to the CEs in the VPN.

When you enable the **Redistribute Connected** option for BGP, the software imports the connected routes (that is, the routes to the directly connected PEs or CEs) to all the other CEs in that particular VPN.

When you enable the Redistribute Connected option, the connected routes (that is, the routes to the directly connected PEs or CEs) are distributed to all the other CEs in that particular VPN. This option is meant for IBGP if the routing protocol between PE-CE is a non-BGP protocol. For example, if the

routing protocol is RIP, OSPF, EIGRP, or Static, the option is meant for the router bgp that is configured on the PE for the MPLS core. On the PE router, there is one router bgp process running at all times for MPLS. This option is also for BGP.

- Step 6** *RIP Metrics (BGP only):* Enter the appropriate RIP metric value. The valid metric values are **1** through **16**.

The metrics used by RIP are hop counts. The hop count for all directly connected interfaces is **1**. If an adjacent router advertises a route to another network with a hop count of 1, then the metric for that network is 2, since the source router must send a packet to that router to get to the destination network.

As each router sends its routing tables to its neighbors, a route can be determined to each network within the AS. If there are multiple paths within the AS from a router to a network, the router selects the path with the smallest hop count and ignores the other paths.

- Step 7** *Redistributed Protocols on PE:* Specify whether you want to redistribute the routing protocols into the PE.

Redistribution allows routing information discovered through another routing protocol to be distributed in the update messages of the current routing protocol. With redistribution, you can reach all the points of your IP internetwork. When a RIP router receives routing information from another protocol, it updates all of its RIP neighbors with the new routing information already discovered by the protocol it imports redistribution information from.

To specify the protocols that RIP needs to import routing information to the PE:

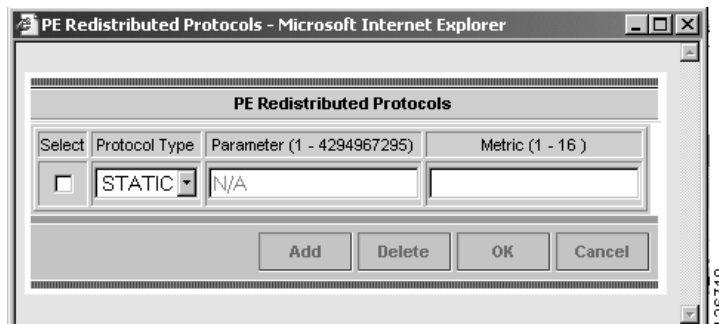
- a. From the **Redistribute Protocols on PE** option, click **Edit**.

The PE Redistributed Protocol dialog box appears.

- b. Click **Add**.

The following dialog box appears (see Figure 5-14).

**Figure 5-14** Selecting Protocols to Redistribute into the PE



- c. From the Protocol Type drop-down list, choose the protocol you want to import into the PE. You can choose one of the following: **Static**, **OSPF**, or **EIGRP**.

- *Redistribute Static*

When you choose **Static** routes for redistribution into RIP, ISC imports the static routes into the PE that is running RIP.

There are no parameters or metrics required for redistributing Static routes into the PE.

- *Redistribute OSPF (Open Shortest Path First)*

When you choose the **OSPF** protocol for redistribution into RIP, ISC imports the OSPF routes into the PE that is running RIP.

**Parameter:** *OSPF process number*

**Metric:** *Any numeral from 1 to 16*

- *Redistribute EIGRP (Enhanced IGRP)*

When you choose the **EIGRP** protocol for redistribution into RIP, ISC imports the EIGRP routes into the PE that is running RIP.

**Parameter:** *EIGRP autonomous system (AS) number*

**Metric:** *Any numeral from 1 to 16*

- Choose the protocol you want to redistribute into RIP on the PE.
- Enter the appropriate parameter for the protocol selected.
- Click **Add**.
- Repeat these steps for any additional protocols you want to redistribute into RIP on the PE, then click **OK**.

**Step 8** *Redistribute Protocols on CE:* Specify whether you want to redistribute the routing protocols into the CE.

To specify the protocols that RIP needs to import routing information to the CE:

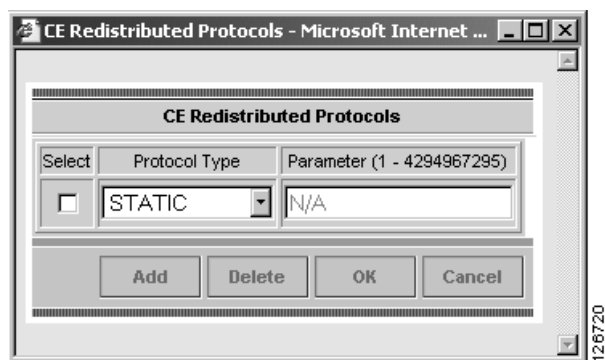
- From the **Redistribute Protocols on CE** option, click **Edit**.

The CE Redistributed Protocol dialog box appears.

- Click **Add**.

The following dialog box appears (see Figure 5-15).

**Figure 5-15** *Selecting Protocols to Redistribute into the CE*



- From the Protocol Type drop-down list, choose the protocol you want to import into the CE.

You can choose one of the following protocols: **Static**, **BGP**, **Connected (routes)**, **IGRP**, **OSPF**, **EIGRP**, or **IS-IS**.

- *Redistribute Static*

When you choose **Static** routes for redistribution into RIP, ISC imports the static routes into the CE that is running RIP.

There are no parameters required for redistributing Static routes into the CE.

- *Redistribute BGP (Border Gateway Protocol)*

When you choose the **BGP** protocol for redistribution into RIP, ISC imports the BGP routes into the CE that is running RIP.

**Parameter:** *BGP autonomous system (AS) number*

- *Redistribute Connected routes*

When you choose the **Connected** routes for redistribution into RIP, ISC imports all the routes to the interfaces connected to the current router. Use the **Connected** option when you want to advertise a network, but you don't want to send routing updates into that network. Note that redistributing connected routes indiscriminately redistributes all connected routes into the routing domain.

**Parameter:** *No parameter required*

- *Redistribute IGRP (Interior Gateway Routing Protocol)*

When you choose the **IGRP** (Interior Gateway Routing) protocol for redistribution into RIP, IP Solution Center imports the IGRP routes into the CE that is running RIP.

**Parameter:** *IGRP autonomous system (AS) number*

- *Redistribute EIGRP (Enhanced IGRP)*

When you choose the **EIGRP** protocol for redistribution into RIP, ISC imports the EIGRP routes into the PE that is running RIP.

**Parameter:** *EIGRP autonomous system (AS) number*

- *Redistribute OSPF (Open Shortest Path First)*

When you choose the **OSPF** protocol for redistribution into RIP, ISC imports the OSPF routes into the CE that is running RIP.

**Parameter:** *OSPF process number*

- *Redistribute IS-IS (Intermediate System-to-Intermediate System)*

When you choose the **IS-IS** protocol for redistribution into RIP, ISC imports the IS-IS routes into the CE that is running RIP.

**Parameter:** *IS-IS tag number*

- Choose the protocol you want to redistribute into RIP on the CE.
- Enter the appropriate parameter for the selected protocol.
- Click **Add**.
- Repeat these steps for any additional protocols you want to redistribute into RIP on the CE, then click **OK**.

**Step 9** When you're satisfied with the RIP protocol settings for this service policy, click **Next**.

To complete this service policy, go to Defining the Service Policy VRF and VPN Information, page 5-39.

## BGP Protocol Chosen

BGP (Border Gateway Protocol) operates over TCP (Transmission Control Protocol), using port 179. By using TCP, BGP is assured of reliable transport, so the BGP protocol itself lacks any form of error detection or correction (TCP performs these functions). BGP can operate between peers that are separated by several intermediate hops, even when the peers are not necessarily running the BGP protocol.

BGP operates in one of two modes: Internal BGP (iBGP) or External BGP (EBGP). The protocol uses the same packet formats and data structures in either case. IBGP is used between BGP speakers within a single autonomous system, while EBGP operates over inter-AS links.

- Step 1** To specify BGP as the routing protocol for the service policy, choose **BGP** from the Routing Protocol drop-down list.

The BGP Routing Protocol dialog box appears (see Figure 5-16).

**Figure 5-16 BGP Selected as the Routing Protocol**

The screenshot shows the 'MPLS Policy Editor - Routing Information' window. On the left, a sidebar lists configuration steps: 1. Policy Type, 2. PE-CE Interface, 3. PE-CE IP Address Scheme, 4. PE-CE Routing Information (selected), and 5. VRF and VPN Membership. The main area is a table with columns 'Attribute', 'Value', and 'Editable'. The 'Routing Protocol' is set to 'BGP'. Other attributes include 'Csc Support', 'Redistribute Static (BGP only)', 'Redistribute Connected (BGP only)', 'CE BGP AS ID' (with value '(1-65535)'), 'Neighbor Allow-AS In' (with value '(1-10)'), 'Neighbor AS Override', and 'Redistributed Protocols on CE'. Most attributes have a checked 'Editable' box. An 'Edit' button is located at the bottom right of the table.

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	BGP	<input checked="" type="checkbox"/>
Csc Support	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CE BGP AS ID:	(1-65535)	<input checked="" type="checkbox"/>
Neighbor Allow-AS In:	(1-10)	<input checked="" type="checkbox"/>
Neighbor AS Override:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistributed Protocols on CE:	<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>

- Step 2** *CSC Support:* To define a Service Policy with Carrier Supporting Carrier (CSC), choose the CSC Support check box from the MPLS Policy Editor - Routing Information. When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service. Provisioning CSC is explained in Chapter 11, “Provisioning Carrier Supporting Carrier.”

- Step 3** *Give Only Default Routes to CE:* Specify whether you want to give only the default routes to the CE.

When you enable the **Give only default routes to CE** option, you indicate whether the site needs *full routing* or *default routing*. Full routing is when the site must know specifically which other routes are present in the VPN. Default routing is when it is sufficient to send all packets that are not specifically for your site to the VPN.

If you choose this option, ISC configures the **default-info originate** command on the PE router under the running protocol (for RIP, OSPF, or EIGRP). For Static, ISC configures an **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** command on the CE router.

- Step 4** *Redistribute Static (BGP Only):* Indicate whether you want to redistribute static routes into BGP.

If you are importing static routes into BGP, choose this check box.

- Step 5** *Redistribute Connected Routes (BGP Only):* Indicate whether you want to redistribute the directly connected routes into BGP.

Enabling the **Redistribute Connected** option imports all the routes to the interfaces connected to the current router. Use the **Redistribute Connected** option when you want to advertise a network, but you don’t want to send routing updates into that network. Note that redistributing connected routes indiscriminately redistributes all connected routes into the routing domain.

When you enable the **Redistribute Connected** option, the connected routes (that is, the routes to the directly connected PE or CE) are distributed to all the other CE in that particular VPN. This option is meant for IBGP if the routing protocol between PE-CE is a non-BGP protocol. For example, if the routing protocol is RIP, OSPF, EIGRP, or Static, the option is meant for the router bgp that is configured on the PE for the MPLS core. On the PE router, there is one router bgp process running at all times for MPLS. This option is also for BGP.

- Step 6** *CE BGP AS ID:* Enter the BGP autonomous system (AS) number for the customer’s BGP network.

The autonomous number assigned here to the CE must be different from the BGP AS number for the service provider’s core network.

- Step 7** *Neighbor Allow-AS In:* If appropriate, enter the **Neighbor Allow-AS-in** value.

When you enter a **Neighbor AllowAS-in** value, you specify a maximum number of times (up to 10) that the service provider autonomous system (AS) number can occur in the autonomous system path.

**Step 8** *Neighbor AS Override:* If required for this VPN, enable the **Neighbor AS Override** option.

The AS Override feature allows the MPLS VPN service provider to run the BGP routing protocol with a customer even if the customer is using the same AS number at different sites. This feature can be used if the VPN customer uses either a private or public autonomous system number.

When you enable the **Neighbor AS-Override** option, you configure VPN Solutions Center to reuse the same AS number on all the VPN's sites.

**Step 9** Specify whether you want to redistribute routing protocols into the CE.

*Redistributed Protocols on CE:* The redistribution of routes into MP-iBGP is necessary only when the routes are learned through any means other than BGP between the PE and CE routers. This includes connected subnets and static routes. In the case of routes learned via BGP from the CE, redistribution is not required because it's performed automatically.

To specify the protocols that BGP needs to import routing information to the CE:

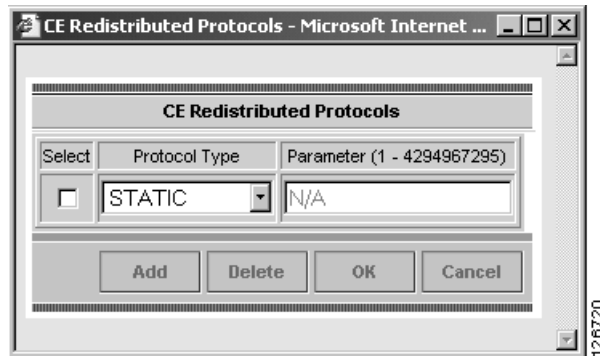
- a. From the **Redistribute Protocols on CE** option, click **Edit**.

The CE Redistributed Protocol dialog box appears.

- b. Click **Add**.

The following dialog box appears (see Figure 5-17).

**Figure 5-17** *Selecting Protocols to Redistribute into the CE*



- c. From the Protocol Type drop-down list, choose the protocol you want to import into the CE.

You can choose one of the following protocols: **Static**, **RIP**, **Connected (routes)**, **IGRP**, **OSPF**, **EIGRP**, or **IS-IS**.

- *Redistribute Static*

When you choose **Static** routes for redistribution into BGP, ISC imports the static routes into the CE that is running BGP.

**Parameter:** *No parameter required*

- *Redistribute RIP (Border Gateway Protocol)*

When you choose the **RIP** protocol for redistribution into BGP, Cisco ISC imports the RIP routes into the CE that is running BGP.

**Parameter:** *No parameter required*

- *Redistribute Connected routes*

When you choose the **Connected** routes for redistribution into BGP, ISC imports all the routes to the interfaces connected to the current router. Use the **Connected** option when you want to advertise a network, but you don't want to send routing updates into that network. Note that redistributing connected routes indiscriminately redistributes all connected routes into the routing domain.

**Parameter:** *No parameter required*

- *Redistribute IGRP (Interior Gateway Routing Protocol)*

When you choose the **IGRP** (Interior Gateway Routing) protocol for redistribution into BGP, IP Solution Center imports the IGRP routes into the CE that is running BGP.

**Parameter:** *IGRP autonomous system (AS) number*

- *Redistribute EIGRP (Enhanced IGRP)*

When you choose the **EIGRP** protocol for redistribution into BGP, ISC imports the EIGRP routes into the CE that is running BGP.

**Parameter:** *EIGRP autonomous system (AS) number*

- *Redistribute OSPF (Open Shortest Path First)*

When you choose the **OSPF** protocol for redistribution into BGP, ISC imports the OSPF routes into the CE that is running BGP.

**Parameter:** *OSPF process number*

- *Redistribute IS-IS (Intermediate System-to-Intermediate System)*

When you choose the **IS-IS** protocol for redistribution into BGP, ISC imports the IS-IS routes into the CE that is running BGP.

**Parameter:** *IS-IS tag number*

- Choose the protocol you want to redistribute into BGP on the CE.
- Enter the appropriate parameter for the selected protocol.
- Click **Add**.
- Repeat these steps for any additional protocols you want to redistribute into BGP on the PE, then click **OK**.

**Step 10** When you're satisfied with the BGP protocol settings for this service policy, click **Next**.

To complete this service policy, go to Defining the Service Policy VRF and VPN Information, page 5-39.

## OSPF Protocol Chosen

The MPLS VPN backbone is not a genuine OSPF area 0 backbone. No adjacencies are formed between PE routers—only between PEs and CEs. MP-iBGP is used between PEs, and all OSPF routes are translated into VPN IPv4 routes. Thus, redistributing routes into BGP does not cause these routes to become external OSPF routes when advertised to other member sites of the same VPN.

**Step 1** To specify OSPF as the routing protocol for the service policy, choose **OSPF** from the Routing Protocol drop-down list.

The OSPF Routing Protocol dialog box appears (see Figure 5-18).

**Figure 5-18 OSPF Selected as the Routing Protocol**

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	OSPF	<input checked="" type="checkbox"/>
CsC Support	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Give Only Default Routes to CE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Static (BGP only)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
OSPF Process ID on PE	(1-65535)	<input checked="" type="checkbox"/>
OSPF Process ID on CE	(1-65535)	<input checked="" type="checkbox"/>
OSPF Area Number or IP Address	(0-4294967295 or a.b.c.d)	<input checked="" type="checkbox"/>
Redistributed Protocols on PE	Edit	<input checked="" type="checkbox"/>
Redistributed Protocols on CE	Edit	<input checked="" type="checkbox"/>

**Step 2** *CsC Support:* To define a Service Policy with Carrier Supporting Carrier (CsC), choose the CsC Support check box from the MPLS Policy Editor - Routing Information. When CsC Support is checked, the CsC functionality is enabled to the MPLS VPN service. Provisioning CsC is explained in Chapter 11, “Provisioning Carrier Supporting Carrier.”

**Step 3** *Give Only Default Routes to CE:* Specify whether you want to give only the default routes to the CE. When you enable the **Give only default routes to CE** option, you indicate whether the site needs *full routing* or *default routing*. Full routing is when the site must know specifically which other routes are present in the VPN. Default routing is when it is sufficient to send all packets that are not specifically for your site to the VPN.

If you choose this option, ISC configures the **default-info originate** command on the PE router under the running protocol RIP or EIGRP and the **default-info originate always** command on the PE router under the running protocol OSPF for Static and configures an **ip route 0.0.0.0 0.0.0.0 <out-going interface name>** command on the CE router.

**Step 4** *Redistribute Static (BGP Only):* Indicate whether you want to redistribute static routes into OSPF.

If you are importing static routes into OSPF, choose this check box.

**Step 5** *Redistribute Connected Routes (BGP Only):* Indicate whether you want to redistribute the directly connected routes into OSPF.

Enabling the **Redistribute Connected** option imports all the routes to the interfaces connected to the current router. Use the **Redistribute Connected** option when you want to advertise a network, but you don't want to send routing updates into that network. Note that redistributing connected routes indiscriminately redistributes all connected routes into the routing domain.

This option is meant for IBGP if the routing protocol between PE-CE is a non-BGP protocol. For example, if the routing protocol is RIP, OSPF, EIGRP, or Static, the option is meant for the router bgp that is configured on the PE for the MPLS core. On the PE router, there is one router bgp process running at all times for MPLS. This option is also for BGP.

**Step 6** *OSPF Process ID on PE:* Enter the OSPF process ID for the PE.

The OSPF process ID is a unique value assigned for each OSPF routing process within a single router—this process ID is internal to the PE only.

**Step 7** *OSPF Process ID on CE:* Enter the OSPF process ID for the CE.

The OSPF process ID is a unique value assigned for each OSPF routing process within a single router—this process ID is internal to the CE only. You can enter this number either as any decimal number from 1 to 65535, or a number in dotted decimal notation.

**Step 8** *OSPF Process Area Number:* Enter the OSPF process area number.

You can enter the OSPF area number for the PE either as any decimal number in the range specified, or a number in dotted decimal notation.

**Step 9** *Redistributed Protocols on PE:* If necessary, specify the redistributed protocols into the PE.



**Note**

Restricting the amount of redistribution can be important in an OSPF environment. Whenever a route is redistributed into OSPF, it is done so as an external OSPF route. The OSPF protocol floods external routes across the OSPF domain, which increases the protocol's overhead and the CPU load on all the routers participating in the OSPF domain.

To specify the protocols that OSPF needs to import to the PE, follow these steps:

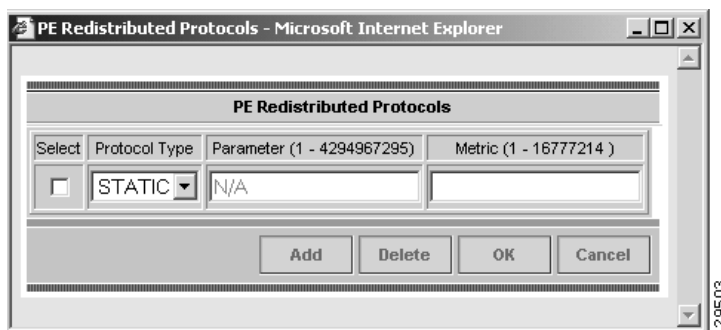
- a. From the **Redistribute Protocols on PE** option, click **Edit**.

The PE Redistributed Protocol dialog box appears.

- b. Click **Add**.

The following dialog box appears (see Figure 5-19).

**Figure 5-19** *Selecting Protocols to Redistribute into the PE*



- c. From the Protocol Type drop-down list, choose the protocol you want to import into the PE.

You can choose one of the following: **Static**, **EIGRP**, or **RIP**.

- *Redistribute Static*

When you choose **Static** routes for redistribution into OSPF, ISC imports the static routes into the PE that is running OSPF.

There are no parameters or metrics required for redistributing Static routes into the PE.

- *Redistribute EIGRP (Enhanced IGRP)*

When you choose the **EIGRP** protocol for redistribution into OSPF, ISC imports the EIGRP routes into the PE that is running OSPF.

**Parameter:** *EIGRP autonomous system (AS) number*

**Metric:** *Any numeral from 1 to 16777214*

- *Redistribute RIP*

When you choose the **RIP** protocol for redistribution into OSPF, ISC imports the RIP routes into the PE that is running OSPF.

**Parameter:** *No parameter required*

**Metric:** Any numeral from 1 to 16777214

- d. Choose the protocol you want to redistribute into OSPF on the PE.
- e. Enter the appropriate parameter for the protocol selected.
- f. Click **Add**.
- g. Repeat these steps for any additional protocols you want to redistribute into OSPF on the PE, then click **OK**.

**Step 10** Specify whether you want to redistribute the routing protocols into the CE.

*Redistribute Protocols on CE:* To specify the protocols that OSPF needs to import routing information to the CE, follow these steps:

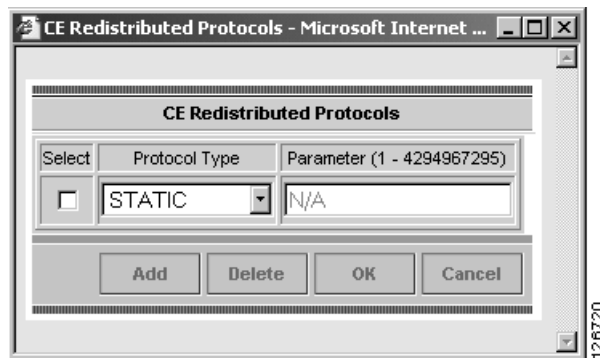
- a. From the **Redistribute Protocols on CE** option, click **Edit**.

The CE Redistributed Protocol dialog box appears.

- b. Click **Add**.

The following dialog box appears (see Figure 5-20).

**Figure 5-20** Selecting Protocols to Redistribute into the CE



- c. From the Protocol Type drop-down list, choose the protocol you want to import into the CE.

You can choose one of the following protocols: **Static**, **RIP**, **BGP**, **Connected (routes)**, **IGRP**, **EIGRP**, or **IS-IS**.

- *Redistribute Static*

When you choose **Static** routes for redistribution into OSPF, ISC imports the static routes into the CE that is running OSPF.

There are no parameters required for redistributing Static routes into the CE.

- *Redistribute RIP*

When you choose the **RIP** protocol for redistribution into OSPF, ISC imports the RIP routes into the CE that is running OSPF.

**Parameter:** No parameter required

- *Redistribute BGP (Border Gateway Protocol)*

When you choose the **BGP** protocol for redistribution into OSPF, ISC imports the BGP routes into the CE that is running OSPF.

**Parameter:** BGP autonomous system (AS) number

- *Redistribute Connected routes*

When you choose the **Connected** routes for redistribution into OSPF, ISC imports all the routes to the interfaces connected to the current router. Use the **Connected** option when you want to advertise a network, but you don't want to send routing updates into that network. Note that redistributing connected routes indiscriminately redistributes all connected routes into the routing domain.

**Parameter:** *No parameter required*

- *Redistribute IGRP (Interior Gateway Routing Protocol)*

When you choose the **IGRP** (Interior Gateway Routing) protocol for redistribution into OSPF, IP Solution Center imports the IGRP routes into the CE that is running OSPF.

**Parameter:** *IGRP autonomous system (AS) number*

- *Redistribute EIGRP (Enhanced IGRP)*

When you choose the **EIGRP** protocol for redistribution into OSPF, ISC imports the EIGRP routes into the CE that is running OSPF.

**Parameter:** *EIGRP autonomous system (AS) number*

- *Redistribute IS-IS (Intermediate System-to-Intermediate System)*

When you choose the **IS-IS** protocol for redistribution into OSPF, ISC imports the IS-IS routes into the CE that is running OSPF.

**Parameter:** *IS-IS tag number*

- Choose the protocol you want to redistribute into OSPF on the CE.
- Enter the appropriate parameter for the selected protocol.
- Click **Add**.
- Repeat these steps for any additional protocols you want to redistribute into OSPF on the CE, then click **OK**.

**Step 11** When you're satisfied with the OSPF protocol settings for this service policy, click **Next**.

To complete this service policy, go to Defining the Service Policy VRF and VPN Information, page 5-39.

## EIGRP Protocol Chosen

Enhanced IGRP (EIGRP) is a hybrid routing protocol that discovers a network like a distance vector protocol (namely IGRP), but maintains a topological database for rapid reconvergence. EIGRP supports variable length subnet masks and discontinuous subnets. When configured for IP, it automatically redistributes routes with IGRP processes defined in the same autonomous system. By default, EIGRP auto-summarizes subnets at the classful network boundaries.

EIGRP performs the same metric accumulation as IGRP. However, if you examine the metric calculation between IGRP and EIGRP, you will see that the EIGRP value is much greater. If you divide the EIGRP metric by 256, you get the same IGRP metric value.

EIGRP allows all routers involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in the recomputation. The result is very fast convergence time.

**Step 1** To specify EIGRP as the routing protocol for the service policy, choose **EIGRP** from the Routing Protocol drop-down list.

The EIGRP Routing Protocol dialog box appears (see Figure 5-21).

**Figure 5-21 EIGRP Selected as the Routing Protocol**

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
<b>Routing Protocol</b>	EIGRP	<input checked="" type="checkbox"/>
CsC Support:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Static (BGP only):	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EIGRP AS ID on PE:	(1-65535)	<input checked="" type="checkbox"/>
EIGRP AS ID on CE:	(1-65535)	<input checked="" type="checkbox"/>
Bandwidth Metric:	(1-4294967295)	<input checked="" type="checkbox"/>
Delay Metric:	(1-4294967295)	<input checked="" type="checkbox"/>
Reliability Metric:	(0-255)	<input checked="" type="checkbox"/>
Loading Metric:	(1-255)	<input checked="" type="checkbox"/>
MTU Metric:	(1-4294967295)	<input checked="" type="checkbox"/>
Redistributed Protocols on PE:	Edit	<input checked="" type="checkbox"/>
Redistributed Protocols on CE:	Edit	<input checked="" type="checkbox"/>

**Step 2** *CsC Support:* To define a Service Policy with Carrier Supporting Carrier (CSC), choose the CSC Support check box from the MPLS Policy Editor - Routing Information. When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service. Provisioning CSC is explained in Chapter 11, “Provisioning Carrier Supporting Carrier.”

**Step 3** *Redistribute Static (BGP only):* If appropriate, enable the **Redistribute Static (BGP only)** option. When you enable the Redistribute Static option for BGP, the software imports the static routes into the core network (running BGP).

**Step 4** *Redistribute Connected (BGP only):* If appropriate, enable the **Redistribute Connected (BGP only)** option. When you enable the **Redistribute Connected** option, the connected routes (that is, the routes to the directly connected PEs or CEs) are distributed to all the other CEs in that particular VPN. This option is meant for IBGP if the routing protocol between PE-CE is a non-BGP protocol. For example, if the routing protocol is RIP, OSPF, EIGRP, or Static, the option is meant for the router `bgp` that is configured on the PE for the MPLS core. On the PE router, there is one router `bgp` process running at all times for MPLS. This option is also for BGP.



**Note**

Redistributing connected routes can be problematic because all the connected routes are redistributed indiscriminately into a specified routing domain. If you do not want all connected routes to be redistributed, use a `distribute-list out` statement to identify the specific connected routes that should be redistributed.

**Step 5** *EIGRP AS ID on PE:* Enter the EIGRP autonomous system ID on the PE. This is a unique 16-bit number.

**Step 6** *EIGRP AS ID on CE:* Enter the EIGRP autonomous system ID on the CE. This is a unique 16-bit number.

**Step 7** Enter the values for the EIGRP metrics as described below.

### EIGRP Metrics

EIGRP uses metrics in the same way as IGRP. Each route in the route table has an associated metric. EIGRP uses a composite metric much like IGRP, except that it is modified by a multiplier of 256. *Bandwidth, Delay, Load, Reliability, and MTU* are the submetrics. Like IGRP, EIGRP chooses a route based primarily on bandwidth and delay, or the composite metric with the lowest numerical value. When EIGRP calculates this metric for a route, it calls it the feasible distance to the route. EIGRP calculates a feasible distance to all routes in the network.

**Bandwidth Metric:** *Bandwidth* is expressed in units of Kilobits. It must be statically configured to accurately represent the interfaces that EIGRP is running on. For example, the default bandwidth of a 56-kbps interface and a T1 interface is 1,544 kbps.

**Delay Metric:** *Delay* is expressed in microseconds. It, too, must be statically configured to accurately represent the interface that EIGRP is running on. The delay on an interface can be adjusted with the **delay time\_in\_microseconds** interface subcommand.

**Reliability Metric:** *Reliability* is a dynamic number in the range of 1 to 255, where 255 is a 100 percent reliable link and 1 is an unreliable link.

**Loading Metric:** *Load* is the number in the range of 1 to 255 that shows the output load of an interface. This value is dynamic and can be viewed using the **show interfaces** command. A value of 1 indicates a minimally loaded link, whereas 255 indicates a link loaded 100 percent.

**MTU Metric:** The maximum transmission unit (MTU) is the recorded smallest MTU value in the path, usually 1500.



#### Note

Whenever you are influencing routing decisions in IGRP or EIGRP, use the Delay metric over Bandwidth. Changing bandwidth can affect other routing protocols, such as OSPF. Changing delay affects only IGRP and EIGRP.

**Step 8** *Redistributed Protocols on PE:* If necessary, specify the redistributed protocols on the PE.

When configured for IP, it automatically redistributes routes with IGRP processes defined in the same autonomous system. By default, EIGRP auto-summarizes subnets at the classful network boundaries.

To specify the protocols that EIGRP needs to import to the PE:

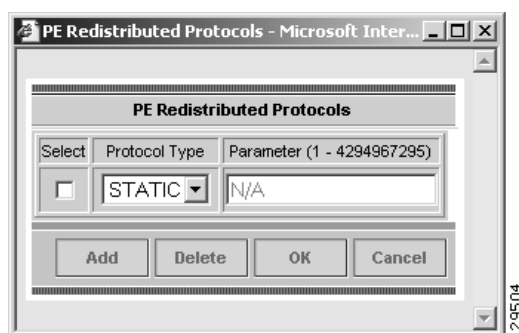
- a. From the **Redistribute Protocols on PE** option, click **Edit**.

The PE Redistributed Protocol dialog box appears.

- b. Click **Add**.

The following dialog box appears (see Figure 5-22).

**Figure 5-22** *Selecting Protocols to Redistribute into the PE*



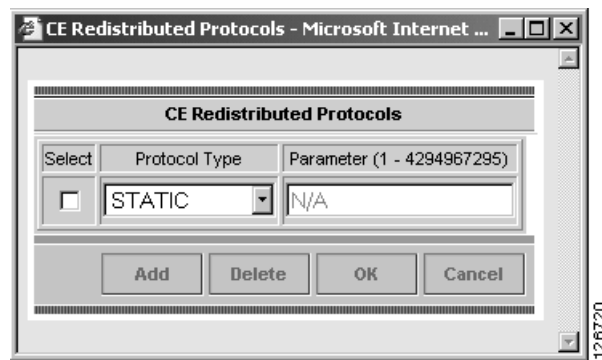
- c. From the Protocol Type drop-down list, choose the protocol you want to import into the PE.  
You can choose one of the following: **Static**, **RIP**, or **OSPF**.
  - *Redistribute Static*  
When you choose **Static** routes for redistribution into EIGRP, ISC imports the static routes into the PE that is running OSPF.  
There are no parameters or metrics required for redistributing Static routes into the PE.
  - *Redistribute RIP*  
When you choose the **RIP** protocol for redistribution into EIGRP, ISC imports the RIP routes into the PE that is running EIGRP.  
**Parameter:** *No parameter required*  
**Metric:** *Any numeral from 1 to 16777214*
  - *Redistribute OSPF (Open Shortest Path First)*  
When you choose the **OSPF** protocol for redistribution into EIGRP, ISC imports the OSPF routes into the PE that is running EIGRP.  
**Parameter:** *OSPF process number*  
**Metric:** *Any numeral from 1 to 16*
- d. Choose the protocol you want to redistribute into EIGRP on the CE.
- e. Enter the appropriate parameter for the protocol selected.
- f. Click **Add**.
- g. Repeat these steps for any additional protocols you want to redistribute into EIGRP on the PE, then click **OK**.

**Step 9** *Redistribute Protocols on CE:* Specify whether you want to redistribute the routing protocols into the CE.

To specify the protocols that EIGRP needs to import routing information to the CE:

- a. From the **Redistribute Protocols on CE** option, click **Edit**.  
The CE Redistributed Protocol dialog box appears.
- b. Click **Add**.  
The following dialog box appears (see Figure 5-23):

**Figure 5-23**      **Selecting Protocols to Redistribute into the CE**



- c. From the Protocol Type drop-down list, choose the protocol you want to import into the CE.

You can choose one of the following protocols: **Static**, **BGP**, **Connected (routes)**, **IGRP**, **RIP**, **OSPF**, or **IS-IS**.

- *Redistribute Static*

When you choose **Static** routes for redistribution into EIGRP, ISC imports the static routes into the CE that is running OSPF.

There are no parameters required for redistributing Static routes into the CE.

- *Redistribute BGP (Border Gateway Protocol)*

When you choose the **BGP** protocol for redistribution into EIGRP, ISC imports the BGP routes into the CE that is running OSPF.

**Parameter:** *BGP autonomous system (AS) number*

- *Redistribute Connected routes*

When you choose the **Connected** routes for redistribution into EIGRP, ISC imports all the routes to the interfaces connected to the current router. Use the **Connected** option when you want to advertise a network, but you don't want to send routing updates into that network. Note that redistributing connected routes indiscriminately redistributes all connected routes into the routing domain.

When you enable the **Redistribute Connected** option, the connected routes (that is, the routes to the directly connected PEs or CEs) are distributed to all the other CEs in that particular VPN. This option is meant for IBGP if the routing protocol between PE-CE is a non-BGP protocol. For example, if the routing protocol is RIP, OSPF, EIGRP, or Static, the option is meant for the router bgp that is configured on the PE for the MPLS core. On the PE router, there is one router bgp process running at all times for MPLS. This option is also for BGP.

**Parameter:** *No parameter required*

- *Redistribute IGRP (Interior Gateway Routing Protocol)*

When you choose the **IGRP** (Interior Gateway Routing) protocol for redistribution into EIGRP, IP Solution Center imports the IGRP routes into the CE that is running EIGRP.

**Parameter:** *IGRP autonomous system (AS) number*

- *Redistribute RIP*

When you choose the **RIP** protocol for redistribution into EIGRP, Cisco ISC imports the RIP routes into the CE that is running EIGRP.

**Parameter:** *No parameter required*

- *Redistribute OSPF (Open Shortest Path First)*

When you choose the **OSPF** protocol for redistribution into EIGRP, ISC imports the OSPF routes into the CE that is running EIGRP.

**Parameter:** *OSPF process number*

- *Redistribute IS-IS (Intermediate System-to-Intermediate System)*

When you choose the **IS-IS** protocol for redistribution into EIGRP, ISC imports the IS-IS routes into the CE that is running EIGRP.

**Parameter:** *IS-IS tag number*

- d. Choose the protocol you want to redistribute into EIGRP on the CE.
- e. Enter the appropriate parameter for the selected protocol.
- f. Click **Add**.

- g. Repeat these steps for any additional protocols you want to redistribute into EIGRP on the CE, then click **OK**.

**Step 10** When you're satisfied with the EIGRP protocol settings for this service policy, click **Next**.

To complete this service policy, go to Defining the Service Policy VRF and VPN Information, page 5-39.

## None Chosen: Cable Services

When operating a cable link, the link does not run a routing protocol. The **None** option in the service policy routing protocol dialog box is provided to allow for configuring a service over a cable link without having to unnecessarily specify a routing protocol.

**Step 1** If this service policy is for cable services, choose **None** from the list of routing protocols.

The following dialog box appears (see Figure 5-24):

**Figure 5-24 No Routing Protocol Selected**

The screenshot shows the 'MPLS Policy Editor - Routing Information' dialog box. On the left, there is a sidebar with a 'Mode: ADDING' button and a list of steps: 1. Policy Type, 2. PE-CE Interface, 3. PE-CE IP Address Scheme, 4. PE-CE Routing Information (selected), and 5. VRF and VPN Membership. The main area contains a table with three columns: Attribute, Value, and Editable. The table has four rows under the 'PE-CE Routing Information' section. The 'Routing Protocol' row has a dropdown menu set to 'NONE'. The 'CsC Support' row has a checked checkbox. The 'Redistribute Static (BGP only)' and 'Redistribute Connected (BGP only)' rows have unchecked checkboxes. The 'Editable' column has checked checkboxes for all rows.

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	NONE	<input checked="" type="checkbox"/>
CsC Support:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Step 2** *CsC Support:* To define a Service Policy with Carrier Supporting Carrier (CSC), choose the CSC Support check box from the MPLS Policy Editor - Routing Information. When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service. Provisioning CSC is explained in Chapter 11, "Provisioning Carrier Supporting Carrier."

**Step 3** *Redistribute Static:* If you want to distribute static routes into the provider core network (which runs BGP), check the **Redistribute Static (BGP only)** check box.

**Step 4** *Redistribute Connected:* Because there is no routing protocol on the cable link, we recommend that you redistribute the connected routes to all the other CEs in the VPN. To do so, check the **Redistribute Connected (BGP only)** check box.

When you enable the **Redistribute Connected** option, the connected routes (that is, the routes to the directly connected PEs or CEs) are distributed to all the other CEs in that particular VPN. This option is meant for IBGP if the routing protocol between PE-CE is a non-BGP protocol. For example, if the routing protocol is RIP, OSPF, EIGRP, or Static, the option is meant for the router bgp that is configured on the PE for the MPLS core. On the PE router, there is one router bgp process running at all times for MPLS. This option is also for BGP.

**Step 5** When finished specifying the necessary settings, click **Next**.

## Defining an MVRFCE PE-CE Service Policy

To define an MVRFCE PE-CE Service Policy, follow these steps:

- Step 1** Log into ISC.
- Step 2** Go to **Service Design > Policies**.

The Policies window appears, as shown in Figure 5-25.

**Figure 5-25 Policies**

**Policies**

Show Policies with  Matching  of Type

Showing 0 of 0 records

#	Policy Name	Type	Owner
---	-------------	------	-------

Rows per page:  Go to page:  of 1

MPLS Policy

- Step 3** From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in Figure 5-26.

**Figure 5-26 MPLS Policy Editor - Policy Type**

**MPLS Policy Editor - Policy Type**

Attribute	Value
<b>Policy Name*:</b>	mvrfce pe-ce
<b>Policy Owner:</b>	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
<b>Customer*:</b>	Cust-A <input type="button" value="Select"/>
<b>Policy Type:</b>	<input type="radio"/> Regular: PE-CE <input checked="" type="radio"/> MVRFCE: PE-CE
<b>CE Present:</b>	<input checked="" type="checkbox"/>

Note: \* - Required Field

- Step 4** Edit the following attributes:
- Step 5** Enter the *policy name*. (**mvrfce pe-ce**)
- Step 6** Choose the Policy Type. (**Regular MVRFCE PE-CE**)
- Step 7** Choose CE Present. (**CE Present**)

**Step 8** Click **Select** to specify a Customer.

The Customer for MPLS Policy ownership window appears, as shown in Figure 5-27.

**Figure 5-27 Customer for MPLS Policy**

116152

**Step 9** Choose a Customer, then click **Select**.

**Step 10** Click **Next**.

The MPLS Policy Editor - PE Interface window appears, as shown in Figure 5-28.

**Figure 5-28 The MPLS Policy Editor - PE Interface**

101675

Attribute	Value	Editable
<b>Reset all Attribute editable flags:</b>		
		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>MVRFCPE PE Facing Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

**Step 11** Click **Next**.

The MPLS Policy Editor - CE Interface window appears, as shown in Figure 5-29.

**Figure 5-29 The MPLS Policy Editor - CE Interface**

**MPLS Policy Editor - Interface**

Attribute	Value	Editable
<b>MVRFCE CE Facing Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
<b>CE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

**Step 12** Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - PE IP Address Scheme window appears, as shown in Figure 5-30.

**Figure 5-30 The MPLS Policy Editor - PE IP Address Scheme**

**MPLS Policy Editor - IP Address Scheme**

Attribute	Value	Editable
<b>PE-MVRFCE Interface Address/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

**Step 13** Check the check box for **Automatically Assign IP Addresses**.

The **IP Address Pool** appears with the **Region Pool** in the window.

**Step 14** Click **Next**.

The MPLS Policy Editor - CE IP Address Scheme window appears, as shown in Figure 5-31.

**Figure 5-31 The MPLS Policy Editor - CE IP Address Scheme**

**MPLS Policy Editor - IP Address Scheme**

Attribute	Value	Editable
<b>MVRFCE-CE Interface Addresses/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Extra CE Loopback Required:	<input type="checkbox"/>	<input type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

**Step 15** Check the check box for **Automatically Assign IP Address**.

**Step 16** Click **Next**.

The MPLS Policy Editor - PE Routing Information window appears, as shown in Figure 5-32.

**Figure 5-32** The MPLS Policy Editor - PE Routing Information

Attribute	Value	Editable
<b>PE-MVRFCE Routing Information</b>		
<b>Routing Protocol</b>	STATIC ▾	<input checked="" type="checkbox"/>
Give Only Default Routes to MVRFCE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

101680

**Step 17** Click **Next** to accept the defaults.

The MPLS Policy Editor - CE Routing Information window appears, as shown in Figure 5-33.

**Figure 5-33** The MPLS Policy Editor - CE Routing Information

<b>MPLS Policy Editor - Routing Information</b>		
Attribute	Value	Editable
<b>MVRFCE-CE Routing Information</b>		
<b>Routing Protocol</b>	STATIC ▾	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

101681

**Step 18** Click **Next** to accept the defaults.



**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - VRF and VPN Membership window appears, as shown in Figure 5-34.

**Figure 5-34** The MPLS Policy Editor - VRF and VPN Membership

**MPLS Policy Editor - VRF and VPN Membership**

Attribute	Value	Editable
<b>VRF Information</b>		
Export Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Import Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Maximum Routes:	(1-4294967295)	<input checked="" type="checkbox"/>
Maximum Route Threshold:	80 (1-100)	<input checked="" type="checkbox"/>
VRF Description:	<input type="text"/>	<input checked="" type="checkbox"/>
Allocate new route distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Template Association</b>		
Template Enable:	<input type="checkbox"/>	
<b>VPN Selection</b>		
PE VPN Membership:		<input checked="" type="checkbox"/>

Select Customer VPN Provider CERC Is Hub

Add Delete

Step 8 of 8 -

< Back Next > Finish Cancel

**Step 19** Click **Next** to accept the defaults.



**Note**

You could add the VPN here, but in this scenario you add the VPN in the Service Request process. Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

**Step 20** Click **Finish**:

The Policies window reappears, as shown in Figure 5-35.

**Figure 5-35** Policies

**Policies**

Show Policies with Policy Name Matching \* of Type All Find

Showing 1 - 1 of 1 record

#	Policy Name	Type	Owner
1.	mvrfce pe-ce	MPLS	Customer - Cust-A

Rows per page: 10 Go to page: 1 of 1 Go

Create Edit Copy Delete

The MVRFCE PE-CE Service Policy is complete.

# Defining the Service Policy VRF and VPN Information

When you are finished defining the routing protocol(s) for this service policy, you must then specify the VRF information.

The MPLS Policy VRF and VPN Membership dialog box appears (see Figure 5-36).

**Figure 5-36** Specifying the VRF Information

Attribute	Value	Editable			
<b>VRF Information</b>					
Export Map:		<input checked="" type="checkbox"/>			
Import Map:		<input checked="" type="checkbox"/>			
Maximum Routes:	(1-4294967295)	<input checked="" type="checkbox"/>			
Maximum Route Threshold:	80 (1-100)	<input checked="" type="checkbox"/>			
VRF Description:		<input checked="" type="checkbox"/>			
Allocate new route distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
VRF And RD Overwrite	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
<b>Template Association</b>					
Template Enable:	<input checked="" type="checkbox"/>				
<b>VPN Selection</b>					
PE VPN Membership:		<input checked="" type="checkbox"/>			
Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	AcmeInc	AcmeIncVPN	FirstProvider	Default	<input checked="" type="checkbox"/>

Add Delete

89753

To specify the VRF and VPN information for this service policy:

**Step 1** *Export Map:* If necessary, enter the name of the export route map.

The name of the export route map you enter here must be the name of an existing export route map on the PE.



**Note**

The Cisco IOS supports only one export route map per VRF (therefore, there can be only one export route map per VPN).

When you use the ISC software to define a management VPN, ISC automatically generates an export route map for the management VPN. Because the Cisco IOS supports only one export route map per VRF and that route map is reserved for the management VPN, the *Export Map* field is not available if the VRF is part of the management VPN.

An export route map does not apply a filter; it can be used to override the default set of route targets associated with a route.

**Step 2** *Import Map:* Enter the name of the import route map.

The name of the import route map you enter here must be the name of an existing import route map on the PE.

**Note**

The Cisco IOS supports only one import route map per VRF—therefore, there can be only one import route map per VPN.

An import route map *does* apply a filter. Therefore, if you want to exclude a particular route from the VRF on this PE, you can either set an export route map on the sending router to make sure it does not have any route targets that can be imported into the current VRF, or create an import route map on the PE to exclude the route.

**Step 3** *Maximum Routes:* Specify the maximum number of routes that can be imported into the VRF on this PE.

**Step 4** *Maximum Route Threshold:* Specify the threshold value for the number of maximum routes. When the specified number of maximum routes is exceeded, ISC sends a warning message.

**Step 5** VRF Description: Optionally, you can enter a description of the VRF for the current VPN.

**Step 6** Allocate New Route Distinguisher: A route distinguisher (RD) is a 64-bit number appended to each IPv4 route that ensures that IP addresses that are unique in the VPN are also unique in the MPLS core. This extended address is also referred to as a VPN-IPv4 address.

When *Allocate new route distinguisher* is enabled, create a new VRF if there is no matching VRF configuration on that PE; otherwise, refuse it.

When *Allocate new route distinguisher* is disabled, find the first matching VRF configuration across the entire range of PEs, regardless of the PE. If this VRF is found on the PE being configured, reuse it. If it isn't found on the PE, create it.

**Note**

The SR might get a VRF that has already been configured on another PE router.

ISC automatically sets the route target (RT) and RD values, but you can assign your own values by checking the VRF and RD check box instead.

**Step 7** *VRF and RD Overwrite:* When you enable the **VRF and RD Overwrite** option, this dialog box presents two new fields (see Figure 5-37) that allow you to overwrite the default VRF name and route distinguisher values.

**Caution**

If not done correctly, changing the default values for the VRF name and the route distinguisher value can alter or disable service requests that are currently running. Please make these changes with caution and only when absolutely necessary.

**Figure 5-37 No Routing Protocol Selected**

VRF And RD Overwrite	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VRF Name:	<input type="text"/>	<input checked="" type="checkbox"/>
RD Value:	<input type="text"/>	<input checked="" type="checkbox"/>

89754

a. *VRF Name:* Enter the new VRF name.

b. *RD Value:* Enter the new RD value.

**Step 8** *Template Enable:* This option determines whether the network devices configured for links within an MPLS service request can be associated with MPLS templates.

When you enable the **Template Enable** option, the next dialog box that appears will let the service operator choose the templates to the associated with the MPLS link.

- Step 9** *PE VPN Membership:* In the **Select** check box, specify the VPN associated with this service policy. The PE VPN Membership information includes the customer name, VPN name, service provider name, CE routing community name, and whether the CERC type is a *hub-and-spoke* CERC or a *fully meshed* CERC.
- If the **Is Hub** check box is checked, it indicates that the CERC type is hub-and-spoke.
- Using the **Add** and **Delete** buttons, you can add a VPN to this list or delete a VPN from this list.
- Step 10** When satisfied with the VRF and VPN selections, click **Finish**.
- 

Now that you have defined a service policy for an MPLS PE-to-CE service, the service operator can now use this policy to create and deploy a service request for a PE-CE link. For details, see Chapter 6, “MPLS VPN Service Requests.”





# MPLS VPN Service Requests

---

This chapter describes how to provision and audit service requests in IP Solution Center (ISC). This chapter contains the following major sections:

- Overview of Service Requests, page 6-1
- Creating Service Requests, page 6-5
- Deploying Service Requests, page 6-33
- Monitoring Service Requests, page 6-35
- Auditing Service Requests, page 6-37
- Editing Configuration Files, page 6-39

## Overview of Service Requests

This section contains the following sections:

- Service Request Transition States, page 6-1
- Service Enhancements, page 6-4
- How ISC Accesses Network Devices, page 6-4
- MPLS VPN Topology Example, page 6-5

## Service Request Transition States

The focus of ISC is the service provided for a customer on the link between a customer CE and a provider PE. The service request model is the centerpiece of service provisioning. With the service request model, the ISC can capture the specified VPN service provisioning request, analyze the validity of the request, and audit the provisioning results.

The service provider operators take all service request information from their customers. ISC can assist the operator in making entries because the product has customer information such as the VPN information, the list of the assigned PEs and CEs, and so forth.

ISC steps the operator through the process and simplifies the task of provisioning the CE and PE by automating most of the tasks required to set up an MPLS VPN.

Figure 6-1 shows a high-level diagram of the relationships and movement among ISC service request states. For a description of the service request transition sequences, see Appendix B, “Service Request Transition States.”

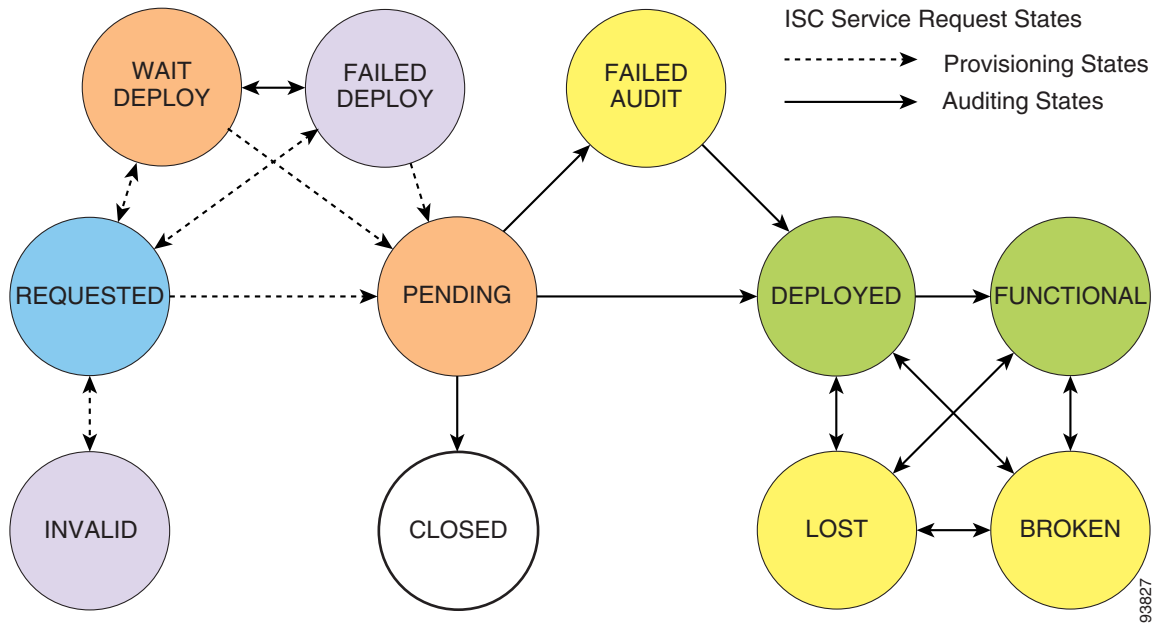
**Figure 6-1** Service Request States: Movement and Relationships

Table 6-1, “Summary of Cisco IP Solution Center Service Request States,” describes each of the service request states and their transition sequences.

**Table 6-1** Summary of Cisco IP Solution Center Service Request States

Service Request Type	Description
<b>Broken</b> (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 <b>Broken</b> if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent.
<b>Closed</b>	A service request moves to <b>Closed</b> if the service request should no longer be used during the provisioning or auditing process. A service request moves to the <b>Closed</b> 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.
<b>Deployed</b>	A service request moves to <b>Deployed</b> if the intention of the service request is found in the router configuration file. <b>Deployed</b> 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.

**Table 6-1 Summary of Cisco IP Solution Center Service Request States (continued)**

<b>Service Request Type</b>	<b>Description</b>
<b>Failed Audit</b>	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 <b>Deployed</b> state. The <b>Failed Audit</b> state is initiated from the <b>Pending</b> state. After a service request is deployed successfully, it cannot re-enter the <b>Failed Audit</b> state (except if the service request is redeployed).
<b>Failed Deploy</b>	The cause for a <b>Failed Deploy</b> 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).
<b>Functional</b> (valid only for L2TPv3 and MPLS services)	An MPLS service request moves to <b>Functional</b> 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.
<b>Invalid</b>	<b>Invalid</b> indicates that the service request information is incorrect in some way. A service request moves to <b>Invalid</b> 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.
<b>Lost</b>	A service request moves to <b>Lost</b> when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the <b>Deployed</b> state, but now some or all router configuration information is missing. A service request can move to the <b>Lost</b> state <i>only</i> when the service request had been <b>Deployed</b> .
<b>Pending</b>	A service request moves to <b>Pending</b> when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. <b>Pending</b> 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.
<b>Requested</b>	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains <b>Requested</b> , the service is in an error state.
<b>Wait Deploy</b>	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. <b>Wait Deploy</b> 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 <b>Wait Deploy</b> state are then downloaded to the Cisco CNS-CE server.

## Service Enhancements

With this release of MPLS VPN Management, a number of enhancements to the service function are available:

- A service is no longer limited to a single PE-CE link at a time. Under ISC, a service can be comprised of multiple PE-CE links per service request.
- Multicast MPLS VPNs

A multicast address is a single address that represents a group of machines. Unlike a broadcast address, however, the machines using a multicast address have all expressed a desire to receive the messages sent to the address. A message sent to the broadcast address is received by all IP-speaking machines, whether they care what it contains or not. For example, some routing protocols use multicast addresses as the destination for their periodic routing messages. This allows machines that have no interest in routing updates to ignore them.

To implement multicast routing, ISC employs the concept of a *multicast domain* (MD), which is a set of VRFs associated with interfaces that can send multicast traffic to each other. A VRF contains VPN routing and forwarding information for unicast. To support multicast routing, a VRF also contains multicast routing and forwarding information; this is called a *Multicast VRF*.

- Site of Origin support

Although a route target provides the mechanisms to identify which VRFs should receive routes, a route target does not provide a facility that can prevent routing loops. These routing loops can occur if routes learned from a site are advertised back to that site. To prevent this, the *Site of Origin* (SOO) feature identifies which site originated the route, and therefore, which site should *not* receive the route from any other PE routers.

- Layer 2 access into MPLS VPNs
- Provisioning PE-Only service requests

## How ISC Accesses Network Devices

When ISC attempts to access a router, it uses the following algorithm:

1. Checks to see if a terminal server is associated with the device, and if this is the case, ISC uses the terminal server to access the device.
2. If there is no terminal server, ISC looks for the management interface on the device.
3. If there is no management interface, ISC tries to access the device using the fully-qualified domain name (hostname plus domain name).

If any step in the VPN Solutions Center device-access algorithm fails, the entire device access operation fails—there is no retry or rollover operation in place. For example, if there is a terminal server and ISC encounters an error in attempting to access the target device through the terminal server, the access operation fails at that point. With the failure of the terminal server access method, ISC does not attempt to find the management interface to access the target device.

# Creating Service Requests

A service request is an instance of service contract between a customer edge router (CE) and a provider edge router (PE). The service request user interface asks you to enter several parameters, including the specific interfaces on the CE and PE routers, routing protocol information, and IP addressing information.

You can also integrate an ISC template with a service request, and 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, “MPLS VPN Service Requests.”

This section has the following sections:

- MPLS VPN Topology Example, page 6-5
- Creating a PE-CE Service Request, page 6-6
- Creating a Multi-VRF Service Request, page 6-17
- Creating a PE-Only Service Request, page 6-26

## MPLS VPN Topology Example

Figure 6-2 shows the topology for the network used to define the service requests in this section.

### PE-CE Example

In the PE-CE example, the service provider needs to create an MPLS service for a CE (mlce1) in their customer site Acme\_NY (in New York).

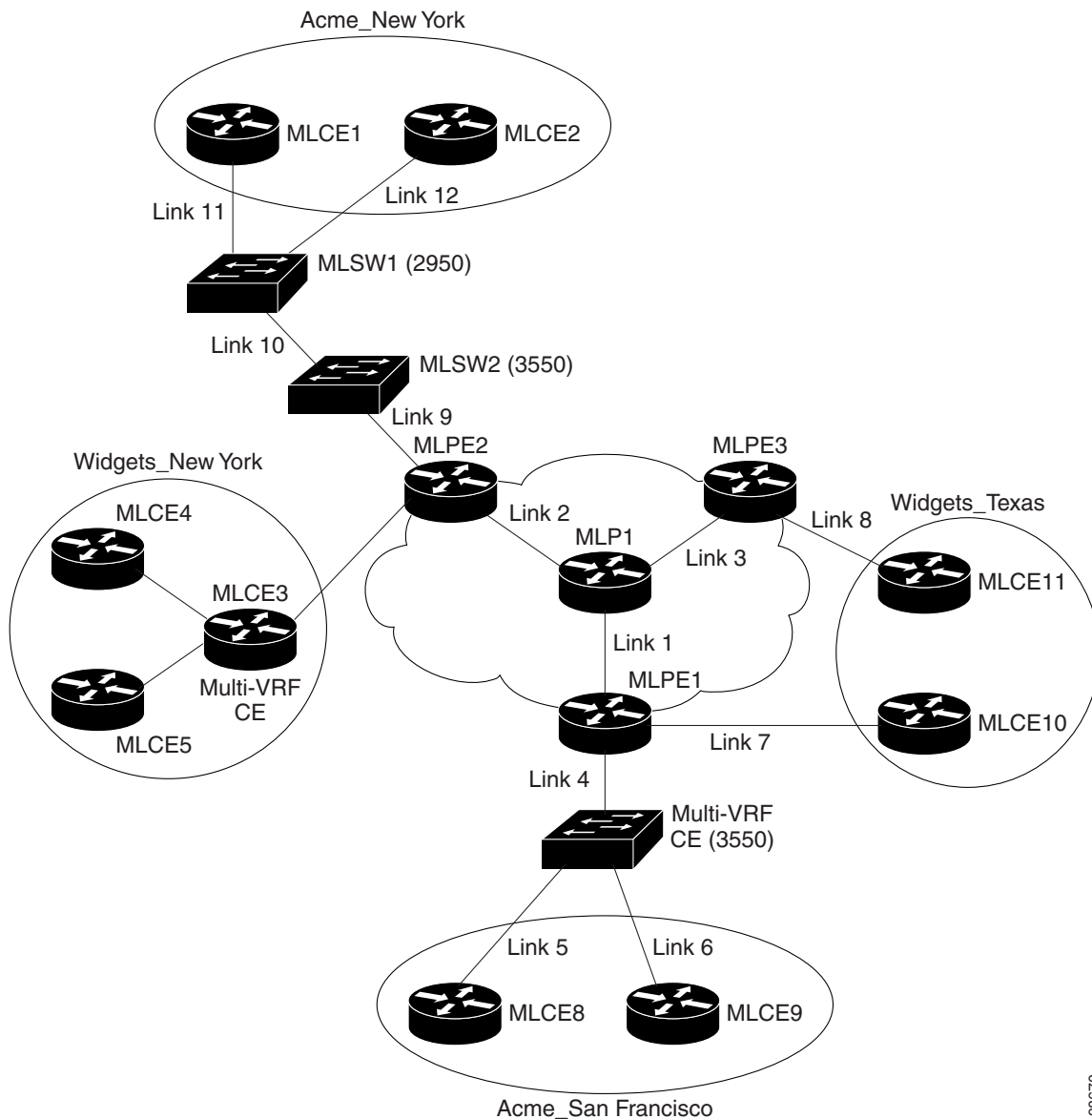
### Multi-VRF Example

In the Multi-VRF example, the service provider needs to create an MPLS service between a CE (mlce4) in their customer site Widgets\_NY (in New York) and a Multi-VRFCE (mlce3) located in their customer site Widgets\_NY (in New York).

The goal is to create a single service request that defines a link between the customer site in New York and the PE (mlpe2).

### PE-Only Example

In the PE-Only example, the service provider needs to create an MPLS service for a PE (mlpe2.)

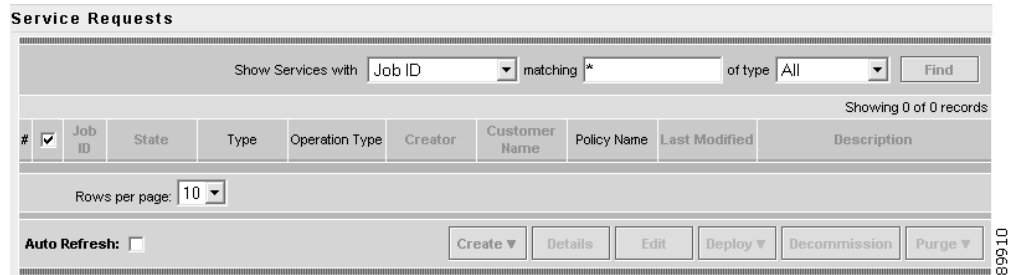
**Figure 6-2 Example Network Topology**

98670

## Creating a PE-CE Service Request

To create a PE-CE service request, follow these steps:

- 
- Step 1** Start up and log in to ISC.
- From the Welcome to ISC window, choose **Service Inventory**.
  - From the Service Inventory window, choose **Inventory and Connection Manager**.
  - From the Inventory and Connection Manager window, choose **Service Requests**.
- The Service Requests dialog box appears (see Figure 6-3).

**Figure 6-3 Initial Service Requests Dialog Box**


**Service Requests**

Show Services with Job ID matching \* of type All Find

Showing 0 of 0 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
Rows per page: 10									

Auto Refresh: ☐

Create Details Edit Deploy Decommission Purge

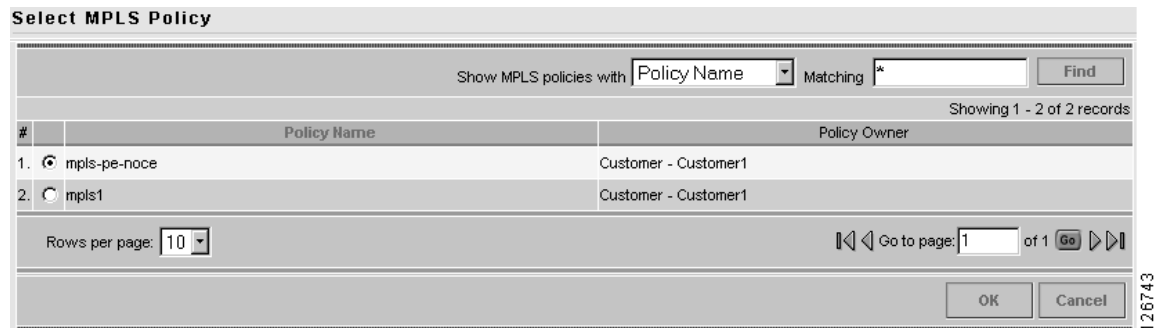
**Step 2** To start the process to create a new service, click **Create**.

A drop-down list is displayed, showing the types of service requests you can create.

**Step 3** Choose **MPLS VPN**.

The Select MPLS Policy dialog box appears (see Figure 6-4).

This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

**Figure 6-4 Selecting the MPLS Policy for This Service**


**Select MPLS Policy**

Show MPLS policies with Policy Name Matching \* Find

Showing 1 - 2 of 2 records

#	Policy Name	Policy Owner
1.	<input checked="" type="radio"/> mpls-pe-noce	Customer - Customer1
2.	<input type="radio"/> mpls1	Customer - Customer1

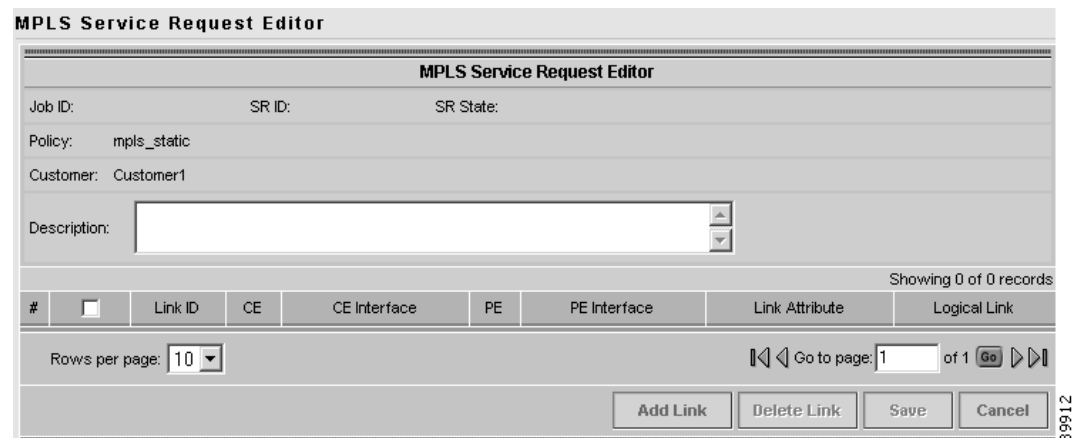
Rows per page: 10

Go to page: 1 of 1 Go

OK Cancel

**Step 4** Choose the policy of choice, then click **OK**.

The MPLS Service Request Editor appears (see Figure 6-5).

**Figure 6-5 MPLS Service Request Editor**


**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: mpls\_static

Customer: Customer1

Description:

Showing 0 of 0 records

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
Rows per page: 10							

Add Link Delete Link Save Cancel

**Step 5** Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields, as shown in Figure 6-6. Notice that the *Select CE* field is enabled. Specifying the CE for the link is the first task required to define the link for this service.

**Figure 6-6** Initial Fields Displayed to Define PE-CE Link

Showing 1-1 of 1 records								
#	<input type="checkbox"/>	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CE	<input type="text"/>	Select PE	<input type="text"/>	Add	N/A

89913

**Step 6** *CE*: Click **Select CE**.

The Select CPE Device dialog box is displayed (see Figure 6-7).

**Figure 6-7** Selecting the CE for the MPLS Link

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	<input checked="" type="radio"/>	mlce1.cisco.com	AcmeInc	Acme_NY	MANAGED
2.	<input type="radio"/>	mlce2.cisco.com	AcmeInc	Acme_NY	MANAGED
3.	<input type="radio"/>	mlce8.cisco.com	AcmeInc	Acme_SF	MANAGED_MGMT_LAN
4.	<input type="radio"/>	mlce9.cisco.com	AcmeInc	Acme_SF	MANAGED
5.	<input type="radio"/>	mlce12.cisco.com	AcmeInc	Acme_TX	MANAGED

89914

- From the *Show CPEs with* drop-down list, you can display CEs by *Customer Name*, by *Site*, or by *Device Name*.
- You can use the **Find** button to either search for a specific CE, or to refresh the display.
- You can set the *Rows per page* to **5**, **10**, **20**, **30**, **40**, or **All**.
- This dialog box displays the first page of the list of currently defined CE devices. The number of pages of information is displayed in the lower right corner of the dialog box.

To go to the another page of CE devices, click the number of the page you want to go to.

**Step 7** In the **Select** column, choose the name of the CE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected CE is now displayed in the *CE* column.

**Step 8** *CE Interface*: Choose the CE interface from the drop-down list (see Figure 6-8).

**Figure 6-8 CE and CE Interface Fields Defined**

Showing 1-1 of 1 records								
#	<input type="checkbox"/>	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	mlce1	FastEthernet0/1	Select PE	<input type="text"/>	Add	N/A

Note that in the PE column, the **Select PE** option is now enabled.

**Step 9** *PE:* Click **Select PE**.

The Select PE Device dialog box is displayed (see Figure 6-9).

**Figure 6-9 Selecting the PE for the MPLS Link**

#	Select	Device Name	Provider Name	Region Name	Role Type
1.	<input type="radio"/>	mlpe1.cisco.com	FirstProvider	US	PE_POP
2.	<input checked="" type="radio"/>	mlpe2.cisco.com	FirstProvider	US	PE_POP
3.	<input type="radio"/>	mlpe3.cisco.com	FirstProvider	US	PE_POP

Rows per page: 10

Select Cancel

- From the *Show PEs with* drop-down list, you can display PEs by *Customer Name*, by *Site*, or by *Device Name*.
- You can use the **Find** button to either search for a specific PE, or to refresh the display.
- You can set the *Rows per page* to **5**, **10**, **20**, **30**, **40**, or **All**.
- This dialog box displays the first page of the list of currently defined PE devices. The number of pages of information is displayed in the lower right corner of the dialog box.

To go to the another page of PE devices, click the number of the page you want to go to.

**Step 10** In the Select column, choose the name of the PE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.

**Step 11** *PE Interface:* Choose the PE interface from the drop-down list (see Figure 6-10).

**Figure 6-10 PE and PE Interface Fields Defined**

Showing 1-1 of 1 records								
#	<input type="checkbox"/>	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	mlce1	FastEthernet0/1	mlpe2	FastEthernet0/1	Add	N/A

Note that the Link Attribute **Add** option is now enabled.

**Step 12** In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor appears, showing the fields for the interface parameters (see Figure 6-11).

**Figure 6-11** Specifying the MPLS Link Interface Attributes

MPLS Link Attribute Editor - Interface	
Attribute	Value
<b>PE Information</b>	
PE	mipe2
Interface Name *	FastEthernet0/1
Interface Description:	
Shutdown Interface:	<input type="checkbox"/>
Encapsulation:	DOT1Q
Auto-Pick Vlan ID:	<input checked="" type="checkbox"/>
<b>CE Information</b>	
CE	mlce1
Interface Name *	FastEthernet0/1
Interface Description:	
Encapsulation:	DOT1Q

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on each of the PE and CE interface fields, see Specifying PE and CE Interface Parameters, page 5-8.



**Note**

The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both.

**Step 13** Edit any interface values that must be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for the IP Address Scheme appears (see Figure 6-12).

**Figure 6-12** Specifying the MPLS Link IP Address Attributes

MPLS Link Attribute Editor - IP Address Scheme	
Attribute	Value
<b>PE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered
Extra CE Loopback Required:	<input type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the IP address scheme fields, see Specifying IP Address Scheme, page 5-12.

**Step 14** Edit any IP address scheme values that must be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for Routing Information appears (see Figure 6-13).

**Figure 6-13** Specifying the MPLS Link Routing Protocol Attributes

**MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	RIP
Give Only Default Routes to CE:	<input type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
RIP Metrics (BGP only):	3 (1-16)
Redistributed Protocols on PE:	Edit
Redistributed Protocols on CE:	Edit

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the routing information for the PE and CE, see *Specifying Routing Protocol for a Service*, page 5-15.

Because the service policy used for this service specified the routing protocol as editable, you can change the routing protocol for this service request as needed.



**Note** For the Static routing protocol, there are two additional attributes that you can add via the Link Attribute Editor. See *Static Routing Protocols*, page 6-14.

- Step 15** Edit any routing protocol values that must be modified for this particular link, then click **Next**. The MPLS Link Attribute Editor for the VRF and VPN attributes appears (see Figure 6-14).

**Figure 6-14** Specifying the MPLS Link VRF and VPN Attributes

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	
Import Map:	
Maximum Routes:	10000 (1-4294967295)
Maximum Route Threshold *:	80 (1-100)
VRF Description:	
Allocate New Route Distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite:	<input type="checkbox"/>
Enable Multicast:	<input checked="" type="checkbox"/>
PIM Mode:	SPARSE_MODE
<b>VPN Selection</b>	
PE VPN Membership *:	
Select	Customer
<input type="checkbox"/>	HMD
VPN	Hameed_MVPN
Provider	AS100
CERC	Default
Is Hub	<input checked="" type="checkbox"/>
<div>Add Delete</div>	

Note: \* - Required Field

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the VRF and VPN information, see *Defining the Service Policy VRF and VPN Information*, page 5-39.

**Step 16** If multicast is enabled, choose the PIM (Protocol Independent Multicast) Mode:

SPARSE\_MODE

SPARSE\_DENSE\_MODE



**Tip**

Multicast routing architecture allows the addition of IP multicast routing on existing IP networks. PIM is an independent unicast routing protocol. It can be operated in two modes: dense and sparse.

**Step 17** Edit any VRF and VPN values that must be modified for this particular link, then click **Finish**.

You return to the MPLS Service Request Editor. You can define multiple links in this service request.

**Step 18** To save your work on this first link in the service request, click **Save**.

You return to the Service Requests dialog box, where the information for the link you just defined is now displayed (see Figure 6-15).

**Figure 6-15 Service Request for an MPLS Link Completed**

The screenshot shows the 'Service Requests' window. At the top, there is a search bar with 'Show Services with' followed by a dropdown menu set to 'Job ID', a text input field containing 'matching \*', and a dropdown menu set to 'of type All'. A 'Find' button is to the right. Below the search bar, it says 'Showing 1-1 of 1 records'. A table with the following columns is displayed: #, Job ID, State, Type, Operation Type, Creator, Customer Name, Policy Name, Last Modified, and Description. The table contains one row: 1, 1, REQUESTED, MPLS, ADD, admin, AcmeInc, acme\_mpls\_pe\_ce, 3/24/03 6:48 PM, and 'Service for link between ml...'. Below the table, there is a 'Rows per page:' dropdown set to '10'. At the bottom, there is an 'Auto Refresh:' checkbox (unchecked) and a row of buttons: 'Create', 'Details', 'Edit', 'Deploy', 'Decommission', and 'Purge'.

As you can see, the service request is in the *Requested* state. When all the links for this service have been defined, you must deploy the service, as described in *Deploying Service Requests*, page 6-33.

## IP Multicast VPN Service Request Configlets







**Step 1** To view the PE and CE configlets for a service request that has been successfully deployed, from the Service Request window, choose the service request you want to see, then click **Details**.

The Service Request Details window appears for the associated job number.

**Step 2** From Service Request Details window, click **Configlets**.

The Service Request Configlets window appears (see Figure 6-16).

**Figure 6-16 Service Request Configlets**

Service Request Configlets	
Configlets for Service Request Job ID 8	
Showing 1 - 2 of 2 records	
#	Device
1.  192.168.133.135	
2.  192.168.133.136	
Rows per page: <input type="text" value="10"/> Go to page: <input type="text" value="1"/> of 1    	
<div>View Configlet</div> <div>OK</div>	

158193

**Step 3** Choose the IP address for the desired configlet, then click **View Configlet**.

Examples of PE and CE configlets are shown below:

### PE Configlet

```

-----
Configlet #1, Job ID 8 (Created: 2006-05-31 17:39:01)
!
ip vrf V2:Hameed_MVPN
rd 100:1011
route-target import 100:12
route-target import 100:13
route-target export 100:12
maximum routes 10000 80
mdt default 239.232.1.1
mdt data 239.232.2.0 0.0.0.255 threshold 50
mdt mtu 1500
!
interface Ethernet1/1.99
description Ethernet1/1.99 dot1q vlan id=99. By VPNSC: Job Id# = 8
encapsulation dot1q 99
ip vrf forwarding V2:Hameed_MVPN
ip address 10.99.0.1 255.255.255.252
ip pim sparse-mode
no shutdown
!
ip multicast vrf V2:Hameed_MVPN route-limit 100000
!
ip multicast-routing vrf V2:Hameed_MVPN
!
ip pim vrf V2:Hameed_MVPN autorp listener
!
ip pim vrf V2:Hameed_MVPN ssm range ssmList
!
ip pim vrf V2:Hameed_MVPN rp-address 10.99.1.2 rp12List
!
ip pim vrf V2:Hameed_MVPN rp-address 10.99.1.5 override
!
ip pim vrf V2:Hameed_MVPN rp-address 10.99.1.1 rp11List override
!
router ospf 21 vrf V2:Hameed_MVPN
redistribute bgp 100 subnets
network 10.99.0.0 0.0.0.3 area 21
!
router bgp 100
address-family ipv4 vrf V2:Hameed_MVPN
redistribute ospf 21 vrf V2:Hameed_MVPN match internal external 1 external 2
exit-address-family
-----

```

**CE Configlet**

-----  
 Configlet #1, Job ID 8 (Created: 2006-05-31 17:39:01)

```
!
interface Ethernet0/0.99
description Ethernet0/0.99 dot1q vlan id=99. By VPNSC: Job Id# = 8
encapsulation dot1Q 99
ip vrf forwarding V2:Hameed_MVPN
ip address 10.99.0.2 255.255.255.252
ip pim sparse-mode
no shutdown
!
router ospf 21
network 10.99.0.0 0.0.0.3 area 21
-----
```

---

**Static Routing Protocols**

For the static routing protocol, in addition to the attributes that you can specify in the service policy, here are two additional attributes that you can add via the Link Attribute Editor.

- **Advertised Routes for CE:** allows you to add a list of ip addresses, static routes to put on the PE, that describes all the address apace in the CE's site.
- **Routes to Reach other Sites:** allows you to add a list of ip addresses, static routes to put on the CE, that describes all the address apace throughout the VPN.

---

**Step 1** When you perform Step 14 on page 4-10 for static routing protocols, the MPLS Link Attribute Editor for Routing Information appears (Figure 6-17).

**Figure 6-17**      **Static Routing Protocol**

The screenshot shows the 'MPLS Link Attribute Editor - Routing Information' window. It contains a table with two columns: 'Attribute' and 'Value'.

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	STATIC
CsC Support:	<input type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
Default Information Originate (BGP only):	<input checked="" type="checkbox"/>
Advertised Routes for CE:	Edit
Routes To Reach Other Sites:	Edit

Note: \* - Required Field

At the bottom, there is a status bar showing '- Step 3 of 4 -' and navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

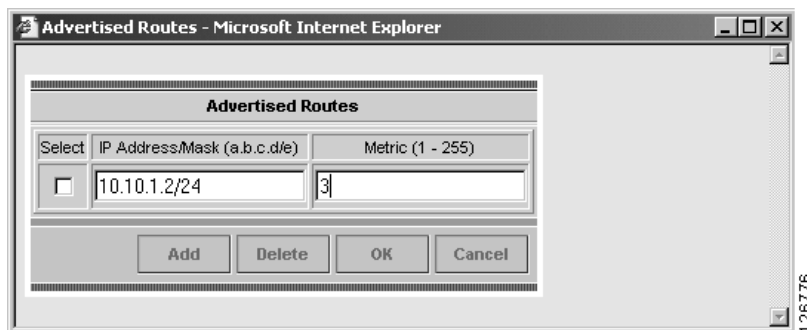
You can edit **Advertised Routes for CE:** and **Routes to Reach other Sites:** for this service request.

**Step 2** To edit **Advertised Routes for CE:**, click **EDIT**. The Advertised Routes window appears as shown in Figure 6-18.

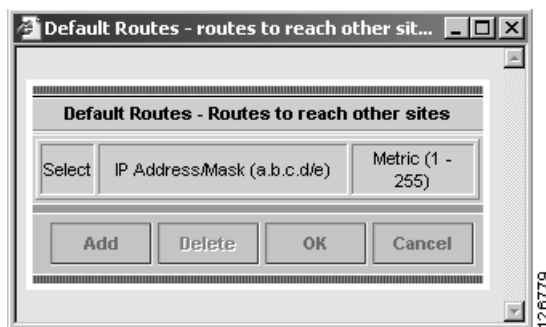
**Figure 6-18**      **Advertised Routes Window**

The screenshot shows a web browser window titled 'Advertised Routes - Microsoft Internet Ex...'. The main content area is titled 'Advertised Routes' and contains a table with two columns: 'Select' and 'IP Address/Mask (a.b.c.d/e)'. Below the table is a 'Metric (1 - 255)' column. At the bottom of the window are four buttons: 'Add', 'Delete', 'OK', and 'Cancel'.

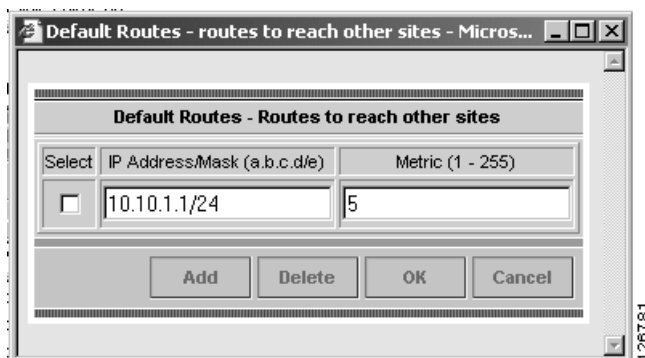
**Step 3** Click **Add** to add IP addresses. The Advertised Routes window appears again as shown in Figure 6-19.

**Figure 6-19 Add IP Address**

- Step 4** Enter an IP address and a metric. Click **Add** to add another IP address or click **OK**.
- Step 5** To edit **Routes to Reach Other Sites**, click **EDIT**. The Routes to reach other sites window appears as shown in Figure 6-20.

**Figure 6-20 Routes to reach other sites Window**

- Step 6** Click **Add** to add IP addresses. The Routes to reach other sites window appears again as shown in Figure 6-21.

**Figure 6-21 Add an IP Address**

- Step 7** Enter an IP address and a metric. Click **Add** to add another IP address or click **OK**.

## Creating a Multi-VRF Service Request

This chapter contains graphics for the following sections:

- Multi-VRF Overview
- Creating an MVRF Service Request

### Multi-VRF Overview

MPLS-VPNs provide security and privacy as traffic travels through the provider network. The CE router has no mechanism to guarantee private networks across the traditional LAN network. Traditionally to provide privacy, either a switch needed to be deployed and each client be placed in a separate VLAN or a separate CE router is needed per each client's organization or IP address grouping attaching to a PE.

These solutions are costly to the customer as additional equipment is needed and requires more network management and provisioning of each client site.

Multi-VRF is a new feature, introduced in Cisco IOS release 12.2(4)T, that addresses these issues. Multi-VRF extends limited PE functionality to a CE router in an MPLS-VPN model. A CE router now has the ability to maintain separate VRF tables in order to extend the privacy and security of an MPLS-VPN down to a branch office rather than just at the PE router node.

CE routers use VRF interfaces to form a VLAN-like configuration on the customer side. Each VRF on the CE router is mapped to a VRF on the PE router. With Multi-VRF, the CE router can only configure VRF interfaces and support VRF routing tables. Multi-VRF extends some of the PE functionality to the CE router—there is no label exchange, there is no LDP adjacency, there is no labeled packet flow between PE and CE. The only PE-like functionality that is supported is the ability to have multiple VRFs on the CE router so that different routing decisions can be made. The packets are sent toward the PE as IP packets.

### Creating an Multi-VRFCE PE-CE Service Request

To create a MVRFCE PE-CE Service Request, follow these steps:

- 
- Step 1** Log into ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.
- The Service Requests window appears, as shown in Figure 6-22.

**Figure 6-22** Service Requests

**Service Requests**

Show Services with Job ID Matching \* of Type All Find

Showing 0 of 0 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
Rows per page: 10 Go to page: 1 of 1 Go									

Auto Refresh: ☐

Create Details Edit Deploy Decommission Purge

MPLS VPN  
L2VPN

116125

- Step 3** From the **Create** drop-down list, choose **MPLS VPN**.  
The Select MPLS Policy window appears, as shown in Figure 6-23.

**Figure 6-23** Select MPLS Policy

**Select MPLS Policy**

Show MPLS policies with Policy Name Matching \* Find

Showing 1 - 1 of 1 record

#	Policy Name	Policy Owner
1.	mvrfce pe-ce	Customer - Cust-A

Rows per page: 10 Go to page: 1 of 1 Go

OK Cancel

116126

- Step 4** Choose the MPLS Policy.
- Step 5** Click **OK**.  
The MPLS Service Request Editor window appears, as shown in Figure 6-24.

**Figure 6-24 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID:                      SR ID:                      SR State:

Policy:    mvrfce pe-ce

Customer: Cust-A

Description:

Showing 0 of 0 records

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE PE Interface	Link Attribute	Logical Link
Rows per page: 10      Go to page: 1 of 1    Go    >>>									

Add Link    Delete Link    Save    Cancel

116127

**Step 6**    Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in Figure 6-25.

**Figure 6-25 MPLS Service Request Editor - Select CE**

Showing 1 - 1 of 1 record

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CE	<input type="text"/>	<input type="text"/>	Select MVRFCE	<input type="text"/>	Select PE	<input type="text"/>	Add	N/A

Rows per page: 10      Go to page: 1 of 1    Go    >>>

Add Link    Delete Link    Save    Cancel

116128

**Step 7**    Click **Select CE**.

The Select CPE Device - CE window appears, as shown in Figure 6-26.

**Figure 6-26 Select CPE Device - CE**

Show CPEs with Customer Name Matching \*    Find

Showing 1 - 1 of 1 record

#	Device Name	Customer Name	Site Name	Management Type
1.	mlce4	Cust-A	Cust-A-Site-mlce4	Unmanaged

Rows per page: 10      Go to page: 1 of 1    Go    >>>

Select    Cancel

116129

**Step 8** Choose the **CPE Device** and then click **Select**.

The MPLS Service Request Editor window appears, as shown in Figure 6-27.

**Figure 6-27 MPLS Service Request Editor - CE Interface**

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce4	FastEthernet0/1		Select MVRFCE		Select PE		Add	N/A

Showing 1 - 1 of 1 record

Rows per page: 10 Go to page: 1 of 1 Go

Add Link Delete Link Save Cancel

**Step 9** Choose the **CE Interface** from the drop-down box.

**Step 10** Click **Select MVRFCE**.

The Select CPE Device - MVRFCE window appears, as shown in Figure 6-28.

**Figure 6-28 Select CPE Device - MVRFCE**

Show CPEs with Customer Name Matching \* Find

#	Device Name	Customer Name	Site Name	Management Type
1.	mlce3	Cust-A	Cust-A-Site-mlce3	Unmanaged Multi-VRF

Showing 1 - 1 of 1 record

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

**Step 11** Choose the **MVRFCE** and then click **Select**.

The MPLS Service Request Editor window appears, as shown in Figure 6-29.

**Figure 6-29 MPLS Service Request Editor - MVRFCE CE Facing Interface**

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Select One	Select PE		Add	N/A

Showing 1 - 1 of 1 record

Rows per page: 10 Go to page: 1 of 1 Go

Add Link Delete Link Save Cancel

**Step 12** Choose the **MVRFCE CE Facing Interface** from the drop-down box.

**Step 13** Choose the **MVRFCE PE Facing Interface** from the drop-down box.

The MPLS Service Request Editor window appears, as shown in Figure 6-30.

**Figure 6-30 MPLS Service Request Editor - Choose MVRFCE PE Facing Interface**

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	Select PE		Add	N/A

Showing 1 - 1 of 1 record

Rows per page: 10 Go to page: 1 of 1

Add Link Delete Link Save Cancel

**Step 14** Click **Select PE**.

The Select PE Device window appears, as shown in Figure 6-31.

**Figure 6-31 Choose PE Device**

Show PEs with Provider Name Matching \* Find

Showing 1 - 3 of 3 records

#	Device Name	Provider Name	Region Name	Role Type
1.	mlpe3	Provider-X	East-X	PE_POP
2.	mlpe4	Provider-X	North-X	PE_POP
3.	mlpe2	Provider-X	West-X	PE_POP

Rows per page: 10 Go to page: 1 of 1

Select Cancel

**Step 15** Choose the **PE** and then click **Select**.

The MPLS Link Attribute Editor window appears, as shown in Figure 6-32.

**Figure 6-32 MPLS Link Attribute Editor - Interface**

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Add	N/A

Showing 1 - 1 of 1 record

Rows per page: 10 Go to page: 1 of 1

Add Link Delete Link Save Cancel

**Step 16** Choose the **PE Interface** from the drop-down box.

**Step 17** Click **Add** in the **Link Attribute** cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 6-32.

**Figure 6-33 MPLS Link Attribute Editor - Interface**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>PE Information</b>	
<b>PE</b>	m1pe2
Interface Name:	FastEthernet0/0. <input type="text"/>
Interface Description:	<input type="text"/>
Shutdown Interface:	<input type="checkbox"/>
Encapsulation:	DOT1Q <input type="button" value="v"/>
VLAN ID *:	510 <input type="text"/> (1-4095)
<b>MVRFCE PE Facing Information</b>	
<b>MVRFCE</b>	m1ce3
Interface Name:	Ethernet0/1. <input type="text"/>
Interface Description:	<input type="text"/>
Encapsulation:	DOT1Q <input type="button" value="v"/>

Note: \* - Required Field

- Step 1 of 7 -

**Step 18** Enter the *VLAN ID* for the PE. (**510**)

**Step 19** Click **Next**.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 6-34.

**Figure 6-34 MPLS Link Attribute Editor - Interface**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>MVRFCE CE Facing Information</b>	
<b>MVRFCE</b>	mlce3
Interface Name:	Ethernet0/2. <input type="text"/>
Interface Description:	<input type="text"/>
Encapsulation:	DOT1Q <input type="button" value="v"/>
VLAN ID *:	530 (1-4095)
<b>CE Information</b>	
<b>CE</b>	mlce4
Interface Name:	FastEthernet0/1. <input type="text"/>
Interface Description:	<input type="text"/>
Encapsulation:	DOT1Q <input type="button" value="v"/>

Note: \* - Required Field

- Step 2 of 7 -

< Back Next > Finish Cancel

**Step 20** Enter the *VLAN ID* for the MVRFCE. (530)

Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 6-35.

**Figure 6-35 MPLS Link Attribute Editor - IP Address Scheme**

**MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>PE-MVRFCE Interface Address/Mask</b>	
IP Numbering Scheme:	IP Numbered <input type="button" value="v"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool <input type="button" value="v"/>

Note: \* - Required Field

**Step 21** Keep the defaults and click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 6-36.

**Figure 6-36 MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>MVRFCE-CE Interface Address/Mask</b>	
IP Numbering Scheme:	IP Numbered ▾
Extra CE Loopback Required:	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool ▾

Note: \* - Required Field

116142

**Step 22** Keep the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 6-37.

**Figure 6-37 MPLS Link Attribute Editor - PE Routing Information**

Attribute	Value
<b>PE-MVRFCE Routing Information</b>	
Routing Protocol	STATIC ▾
Give Only Default Routes to MVRFCE:	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>
Advertised Routes for MVRFCE:	Edit
Routes To Reach Other Sites:	Edit

Note: \* - Required Field

116143

**Step 23** Keep the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 6-38.

**Figure 6-38 MPLS Link Attribute Editor - MVRFCE Routing Information**

Attribute	Value
<b>MVRFCE-CE Routing Information</b>	
Routing Protocol	STATIC ▾
Give Only Default Routes to CE:	<input type="checkbox"/>
Advertised Routes for CE:	Edit
Routes To Reach Other Sites:	Edit

Note: \* - Required Field

116144

**Step 24** Keep the defaults and click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears (not shown).

**Step 25** Click **Add** to choose a VPN.

The Choose VPN window appears, as shown in Figure 6-39.

**Figure 6-39 Choose VPN**

Customer:  VPN:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Customer	VPN	Provider	CERC	Topology
1.	<input type="checkbox"/>	CUST-A	west-xVPN	PROVIDER-X	Default	Hub and Spoke

Rows per page:  Go to page:  of 1

**Step 26** Choose a VPN.

**Step 27** Click **Join as Hub** or **Join as Spoke** to join the CERC.

**Step 28** Click **Done**.

The MPLS Link Attribute Editor - VRF and VPN window reappears, as shown in Figure 6-40.

**Figure 6-40 MPLS Service Request Editor**

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	<input type="text"/>
Import Map:	<input type="text"/>
Maximum Routes:	<input type="text"/> (1-4294967295)
Maximum Route Threshold *:	<input type="text" value="80"/> (1-100)
VRF Description:	<input type="text"/>
Allocate new route distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	

Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	CUST-A	west-xVPN	PROVIDER-X	Default	<input checked="" type="checkbox"/>

Note: \* - Required Field

- Step 7 of 7 -

**Step 29** Click **Finish**.

The MPLS Service Request Editor window appears, as shown in Figure 6-41.

**Figure 6-41 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID: 7      SR ID: 8      SR State: REQUESTED

Policy: mpls-mvrfce-pe-ce

Description: mpls-mvrfce-pe-ce

Showing 1-1 of 1 records

#	Link ID	CE	CE Interface	MVRFCFCE CE Facing Interface	MVRFCFCE	MVRFCFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	6	m1ce4	FastEthernet0/1	Ethernet0/2	m1ce3	Ethernet0/1	m1pe2	FastEthernet0/0	Edited	Details...

Rows per page: 10      Go to page: 1 of 1

Add Link   Delete Link   Save   Cancel

**Step 30** Enter the Service Request *description* and then click **Save**. (mpls-mvrfce-pe-ce)

The MPLS Service Requests window appears, as shown in Figure 6-42.

**Figure 6-42 Service Request**

**Service Requests**

Show Services with Job ID Matching \*      of Type All      Find

Showing 1 - 1 of 1 record

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	1	REQUESTED	MPLS	ADD	admin	Cust-A	mvrfcfce-pe-ce	2/22/04 7:24 PM	mpls-mvrfce-pe-ce service re...

Rows per page: 10      Go to page: 1 of 1

Auto Refresh: ☒      Create   Details   Edit   Deploy   Decommission   Purge

The MPLS VPN MVRFCFCE PE-CE Service Request is in the Requested state and ready to deploy.

## Creating a PE-Only Service Request

To create a PE-Only (No CE) service request, follow these steps:

- Step 1** Start up and log in to ISC.
- From the Welcome to ISC window, choose **Service Inventory**.
  - From the Service Inventory window, choose **Inventory and Connection Manager**.
  - From the Inventory and Connection Manager window, choose **Service Requests**.
- The Service Requests dialog box appears (see Figure 6-43).

**Figure 6-43 Initial Service Requests Dialog Box**


**Service Requests**

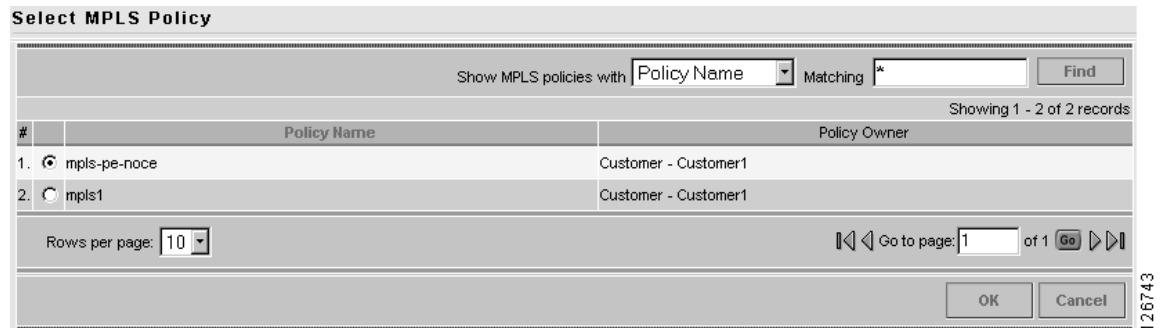
Show Services with Job ID matching \* of type All Find

Showing 0 of 0 records

#	<input checked="" type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
Rows per page: 10										
Auto Refresh: <input checked="" type="checkbox"/> Create Details Edit Deploy Decommission Purge										

- Step 2** To start the process to create a new service, click **Create**.  
A drop-down list is displayed, showing the types of service requests you can create.

- Step 3** Choose **MPLS VPN**.  
The Select MPLS Policy dialog box appears (see Figure 6-44).  
This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

**Figure 6-44 Selecting the PE-Only Policy for this Service**


**Select MPLS Policy**

Show MPLS policies with Policy Name Matching \* Find

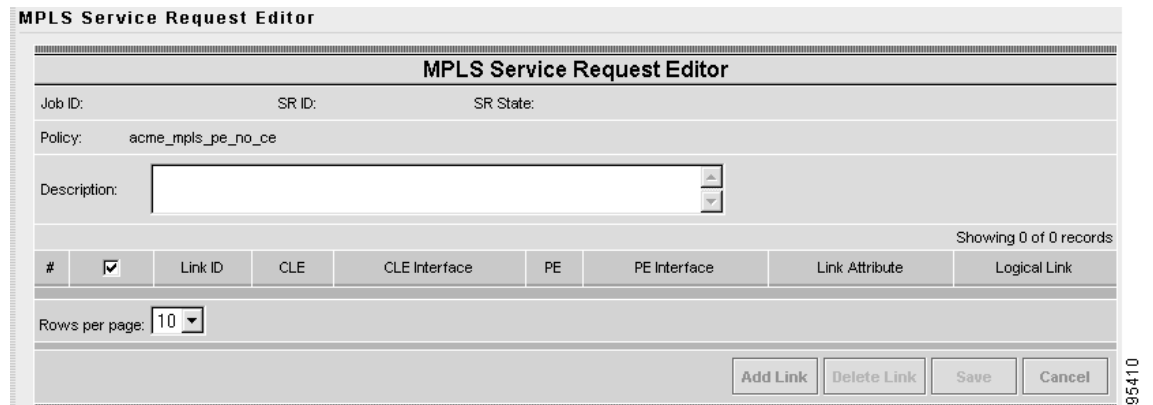
Showing 1 - 2 of 2 records

#		Policy Name	Policy Owner
1.	<input checked="" type="radio"/>	mpls-pe-noce	Customer - Customer1
2.	<input type="radio"/>	mpls1	Customer - Customer1

Rows per page: 10 Go to page: 1 of 1 Go

OK Cancel

- Step 4** Choose the policy that has CE not present, then click **OK**.  
The MPLS Service Request Editor appears (see Figure 6-45).

**Figure 6-45 MPLS Service Request Editor**


**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: acme\_mpls\_pe\_no\_ce

Description:

Showing 0 of 0 records

#	<input checked="" type="checkbox"/>	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
Rows per page: 10								
Add Link Delete Link Save Cancel								

**Step 5** Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields, as shown in Figure 6-46. Notice that the *Select PE* field is enabled. Specifying the PE for the link is the first task required to define the link for this service, unless a CLE switch link is needed. If a CLE switch is needed go to “Adding a CLE Service Request” section on page 6-33.

**Figure 6-46** Initial Fields Displayed to Define PE-Only Link

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="text"/>	Select PE	<input type="text"/>	Add	N/A

Rows per page: 10

Add Link Delete Link Save Cancel

**Step 6** *PE*: Click **Select PE**.

The Select PE Device dialog box is displayed (see Figure 6-47).

**Figure 6-47** Selecting the PE for the PE-Only Link

PE for MPLS VPN Link

Show PEs with Provider Name matching First\* Find

Showing 1-4 of 4 records

#	Select	Device Name	Provider Name	Region Name	Role Type
1.	<input type="radio"/>	mlpe1.cisco.com	FirstProvider	US	PE_POP
2.	<input checked="" type="radio"/>	mlpe2.cisco.com	FirstProvider	US	PE_POP
3.	<input type="radio"/>	mlpe3.cisco.com	FirstProvider	US	PE_POP
4.	<input type="radio"/>	mlpe4.cisco.com	FirstProvider	US	PE_POP

Rows per page: 10

Select Cancel

- From the *Show PEs with* drop-down list, you can display PEs by *Provider Name*, by *Region*, or by *Device Name*.
- You can use the **Find** button to either search for a specific PE, or to refresh the display.
- You can set the *Rows per page* to **5, 10, 20, 30, 40**, or **All**.
- This dialog box displays the first page of the list of currently defined PE devices. The number of pages of information is displayed in the lower right corner of the dialog box.

To go to the another page of PE devices, click the number of the page you want to go to.

**Step 7** In the **Select** column, choose the name of the PE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.

*PE Interface*: Choose the PE interface from the drop-down list (see Figure 6-48).

**Figure 6-48** PE and PE Interface Fields Defined

**MPLS Service Request Editor**

Job ID:                      SR ID:                      SR State:

Policy:      acme\_mpls\_pe\_no\_ce

Description:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="text"/>	mlpe2	Serial3/1	Add	N/A

Rows per page:

95413

Note that the Link Attribute **Add** option is now enabled.

**Step 8** In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor is displayed, showing the fields for the interface parameters (see Figure 6-49).

**Figure 6-49** Specifying the PE-Only Link Interface Attributes

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>PE Information</b>	
PE	mlpe4
Interface Name:	Ethernet1/2. <input type="text"/> (1-4294967295)
Interface Description:	<input type="text"/>
Shutdown Interface:	<input type="checkbox"/>
Encapsulation:	DOT1Q <input type="button" value="v"/>
VLAN ID *:	<input type="text"/> (1-4095)
Auto-Pick VLAN ID:	<input type="checkbox"/>
Use SVI:	<input type="checkbox"/>
Link Speed:	None <input type="button" value="v"/>
Link Duplex:	None <input type="button" value="v"/>
ETTH Support:	<input type="checkbox"/>
Standard UNI Port:	<input checked="" type="checkbox"/>
<b>UNI Security Information</b>	
Disable CDP:	<input type="checkbox"/>
Filter BPDU:	<input type="checkbox"/>
Use Existing ACL Name:	<input type="checkbox"/>
UNI MAC Addresses:	<input type="button" value="Edit"/>
UNI Port Security:	<input checked="" type="checkbox"/>
Maximum MAC Address:	<input type="text"/> (1 - 5120)
Aging (in minutes):	<input type="text"/> (0 - 1440)
Violation Action:	PROTECT <input type="button" value="v"/>
Secure MAC Addresses:	<input type="button" value="Edit"/>
<b>CE Information</b>	
CE	mlce2
Interface Name:	FastEthernet0/1. <input type="text"/> (1-4294967295)
Interface Description:	<input type="text"/>
Encapsulation:	DOT1Q <input type="button" value="v"/>

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the PE interface fields, see *Specifying PE and CE Interface Parameters*, page 5-8.

- Step 9** Edit any interface values that must be modified for this particular link, then click **Next**.  
The MPLS Link Attribute Editor for the IP Address Scheme appears (see Figure 6-50).

**Figure 6-50** Specifying the PE-Only Link IP Address Attributes

**MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>PE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered <input type="button" value="v"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool <input type="button" value="v"/>

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the IP address scheme fields, see *Specifying IP Address Scheme*, page 5-12.

- Step 10** Edit any IP address scheme values that must be modified for this particular link, then click **Next**.  
The MPLS Link Attribute Editor for Routing Information appears (see Figure 6-51).

**Figure 6-51** Specifying the PE-Only Routing Protocol Attributes

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	BGP
CsC Support:	<input type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
Site of Origin:	<input checked="" type="checkbox"/>
Value *	Select
Neighbor IP Address *	<input type="text"/> (a.b.c.d)
CE BGP AS ID *	<input type="text"/> (1-65535)
Neighbor Allow-AS in:	<input type="text"/> (1-10)
Neighbor AS Override:	<input type="checkbox"/>

Note: \* - Required Field

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the routing information for the PE, see *Specifying Routing Protocol for a Service*, page 5-15.

Because the service policy used for this service specified the routing protocol as editable, you can change the routing protocol for this service request as needed.

- Step 11** If you check **Site of Origin**, the screen updates to include the required step of selecting a value:
- Click **Select**.  
The Site for SOO Value window appears.
  - From the available list shown, check the check box associated with a site and its SOO value, then click **Select**.
- Step 12** Edit any routing protocol values that must be modified for this particular link, then click **Next**.  
The MPLS Link Attribute Editor for the VRF and VPN attributes appears (see Figure 6-52).

**Figure 6-52** Specifying the PE-Only Link VRF and VPN Attributes

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	<input type="text"/>
Import Map:	<input type="text"/>
Maximum Routes:	<input type="text"/> (1-4294967295)
Maximum Route Threshold *:	<input type="text"/> 80 (1-100)
VRF Description:	<input type="text"/>
Allocate new route distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	
Select	Customer
<input type="checkbox"/>	AcmeInc
VPN	AcmeIncVPN
Provider	FirstProvider
CERC	Default
Is Hub	<input checked="" type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the VRF and VPN information, see *Defining the Service Policy VRF and VPN Information*, page 5-39.

**Step 13** Edit any VRF and VPN values that must be modified for this particular link, then click **Finish**.

You return to the MPLS Service Request Editor. You can define multiple links in this service request.

**Step 14** To save your work on this first link in the service request, click **Save**.

You return to the Service Requests dialog box, where the information for the link you just defined is now displayed (see Figure 6-53).

**Figure 6-53** Service Request for an PE-Only Link Completed

**Service Requests**

Show Services with  matching  of type

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	<input type="checkbox"/>	11	REQUESTED	MPLS	ADD	admin	AcmeInc	acme_mpls_pe_no_ce	6/18/03 3:00 PM	

Rows per page:

Auto Refresh: ☒

You can add additional links to this service request by choosing **Add Link** and specifying the attributes of the next link in the service. As you can see, the service request is in the *Requested* state. When all the links for this service have been defined, you must deploy the service, as described in *Deploying Service Requests*, page 6-33.

## Adding a CLE Service Request

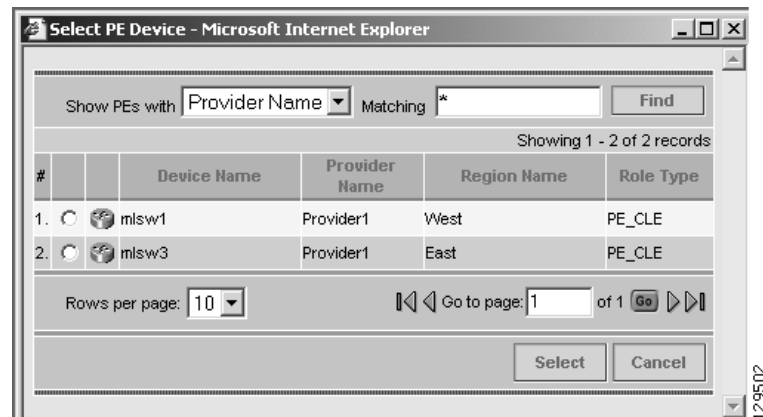
To add a CLE link:

**Step 1** Follow Step 1 through Step 5 of “Creating a PE-Only Service Request” section on page 6-26.

**Step 2** Click **Select CLE**.

The Select PE Device dialog box is displayed (see Figure 6-54).

**Figure 6-54** Selecting the CLE for the PE-Only Link



- From the *Show PEs with* drop-down list, you can display PEs by *Provider Name*, by *Region*, or by *Device Name*.
- You can use the **Find** button to either search for a specific PE, or to refresh the display.
- You can set the *Rows per page* to **5**, **10**, **20**, **30**, **40**, or **All**.
- This dialog box displays the first page of the list of currently defined PE devices. The number of pages of information is displayed in the lower right corner of the dialog box.

To go to the another page of PE devices, click the number of the page you want to go to.

**Step 3** In the Select column, choose the name of the CLE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected CLE is now displayed in the CLE column.

**Step 4** *CLE Interface*: Choose the CLE interface from the drop-down list.

**Step 5** Continue following Step 8 through Step 13 of “Creating a PE-Only Service Request” section on page 6-26.

## Deploying Service Requests

When you have queued one or more service requests, you can then deploy them. This procedure automatically audits the new service requests. This audit passes the service request into an operational state.

ISC sets up a scheduled task that deploys service requests to the appropriate routers. This involves computing the configlets for each service request, downloading the configlets to the routers, and running audit reports to determine whether the service was successfully deployed.

You can choose to deploy the service requests immediately or schedule their deployment.

- Step 1** Start up and log in to ISC.
- From the Welcome to ISC window, choose **Service Inventory**.
  - From the Service Inventory window, choose **Inventory and Connection Manager**.
  - From the Inventory and Connection Manager window, choose **Service Requests**.

The Service Requests dialog box appears (see Figure 6-55).

**Figure 6-55** Selecting a Service Requests to Deploy

Service Requests

Show Services with Job ID matching \* of type All Find

Showing 1-1 of 1 records

#	<input checked="" type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	<input checked="" type="checkbox"/>	1	REQUESTED	MPLS	ADD	admin	AcmeInc	acme_mpls_pe_ce	3/24/03 6:48 PM	Service for link between ml...

Rows per page: 10

Auto Refresh: ☒

Create Details Edit Deploy Decommission Purge

- Step 2** Check the check box next to the Job ID for the service request you want to deploy.

- Step 3** Click the **Deploy** drop-down list.

You have two deployment options, as shown in Figure 6-56:

- Deploy*: Use **Deploy** when the service request state is *Requested* or *Invalid*.
- Force Deploy*: Use **Force Deploy** when the service request state is *Deployed* or *Failed Audit*.

**Figure 6-56** Deployment Options

Auto Refresh: ☐

Create Details Edit Deploy Decommission Purge

Deploy  
Force Deploy

- Step 4** Choose **Deploy**.

The Deploy Service Requests dialog box appears, which allows you to schedule when you want to deploy the selected service request (see Figure 6-57).

**Figure 6-57** Scheduling a Service Request for Deployment

**Deploy Service Requests**

Task Name \*: Task Created 2003-08-25 14:20:35.37

Task Type: Deployment

Task Description: Created on Mon Aug 25 14:20:35 PST 2003

Single Run: ☐ Now ☐ Once

Periodic Run: ☐ Minute ☐ Hourly ☒ Daily ☐ Weekly ☐ Monthly

Periodic Run Attributes

Run Interval: Every 1 day(s)

Run Limits: Maximum Runs: unlimited Maximum Running Instances: unlimited

Start Date and Time

Date: August 25 2003

Time: 6 00 PM

End Date and Time (Default is unlimited)

Date: August 29 2003

Time: 6 00 PM

Save Cancel

**Step 5** Complete the fields in this dialog box to schedule the service requested as needed.

**Step 6** When satisfied with the schedule settings, click **Save**.

You return to the Service Requests dialog box. Check the Status display in the lower left corner of the window. If the service request has been deployed successfully, the Status display appears as shown in Figure 6-58.

**Figure 6-58** Status for Successful Deployment

**Status**

Operation: Deploy Service Requests

Status: ☒ Succeeded

**Step 7** To update the State from *Requested* to *Deployed*, enable the Auto Refresh check box.

You can view logs to check on the task status and whether or not it completed successfully. To view logs, choose **Monitoring > Task Manager > Logs** (for Log details, refer to *Cisco IP Solution Center Infrastructure Reference* on Cisco.com).

## Monitoring Service Requests

Once you have created and deployed a service request, you can monitor its status.

- Step 1** Click the **Monitoring** tab.
- Step 2** From the Monitoring window, choose **Task Manager**.  
The Task Manager dialog box is displayed (see Figure 6-59).

**Figure 6-59 Viewing Information on Running Tasks**

**Tasks**

Show Tasks with Task Name matching \* of Type \*

Showing 1 - 10 of 11 records

#	<input type="checkbox"/>	Task Name	Type	Schedule	Creator	Created on
1.	<input type="checkbox"/>	Task Created 2004-09-28 10:07:55.103	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD	2004-09-28 10:07:57.424
2.	<input type="checkbox"/>	Task Created 2004-09-28 10:03:09.686	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD	2004-09-28 10:03:14.736
3.	<input type="checkbox"/>	Task Created 2004-09-28 09:58:02.981	Service Deployment	Single run at 2004-09-28 09:58:00.0	SD	2004-09-28 09:58:05.343
4.	<input type="checkbox"/>	Task Created 2004-09-28 09:51:34.271	Service Deployment	Single run at 2004-09-28 09:51:00.0	SD	2004-09-28 09:51:37.044
5.	<input type="checkbox"/>	Collect Config 2004-09-27 17:05:47.503	Collect Config	Single run at 2004-09-27 17:06:00.0	ENG	2004-09-27 17:05:50.164
6.	<input type="checkbox"/>	Task Created 2004-09-22 11:37:56.332	Service Deployment	Single run at 2004-09-22 11:37:00.0	SD	2004-09-22 11:37:58.719
7.	<input type="checkbox"/>	Task Created 2004-09-22 11:35:10.21	Service Deployment	Single run at 2004-09-22 11:35:00.0	SD	2004-09-22 11:35:12.59
8.	<input type="checkbox"/>	Task Created 2004-09-22 11:29:16.333	Service Deployment	Single run at 2004-09-22 11:29:00.0	SD	2004-09-22 11:29:18.964
9.	<input type="checkbox"/>	Task Created 2004-09-22 11:24:33.102	Service Deployment	Single run at 2004-09-22 11:24:00.0	SD	2004-09-22 11:24:36.146
10.	<input type="checkbox"/>	Task Created 2004-09-22 11:17:14.623	Service Deployment	Single run at 2004-09-22 11:17:00.0	SD	2004-09-22 11:17:22.207

Rows per page:

Auto Refresh: ☒

- Step 3** Check the check box for the task (that is, service request) that you're interested in.
- Step 4** To see details about the service request's deployment, click **Details**.  
The Service Request Details window appears (see Figure 6-60).

**Figure 6-60 Service Request Details Displayed**

**View Task Details**

Task Name:	Task Created 2004-09-22 11:17:14.623
Task Owner:	none
Action:	com.cisco.vpnsc.prov.provdrv.ProvDrv
Targets:	
IsForceRedeploy:	false
IsProvision:	true
ipsec-rekey:	false
JobIdList:	1
Action:	com.cisco.vpnsc.prov.provdrv.ProvDrv
Targets:	
IsProvision:	false
JobIdList:	1
JITUpload:	false

# Auditing Service Requests

This section describes auditing in MPLS VPN. It contains the following sections:

- Functional Audit, page 6-37
- Configuration Audit, page 6-38

## Functional Audit

A functional audit verifies that the links in a service request or VPN are working correctly. The audit checks the routes to remote CEs in the VRF route tables on the PE devices. The user can optionally ping the connected CE from the PE to verify that the link is functional.

## How to Perform a Functional Audit

ISC automatically provides a functional audit whenever a service request is deployed or force-redeployed.

You can also create a task to do a functional audit for one or more service requests. To create a task to do a functional audit, follow these steps:

- 
- Step 1** Go to **Monitoring > Tasks > Audit > MPLS Functional Audit**
- Step 2** Choose one or more service requests in Deployed, Functional, or Broken states as the targets for the task.
- a. You can choose a VPN to audit. If you choose a VPN to audit, all the links that form the VPN are audited.
  - b. You can choose either SR(s) or VPN(s) in one task, but you cannot choose both in the same task.
  - c. After the audit, a schedule page appears.
  - d. You can choose a schedule.
  - e. In the summary page, you can un-check the Perform Ping to verify PE/CE link check box if you do not want to invoke ping in that particular task.
  - f. For links without CEs (CE not present case), ping is not performed, whether the check box is selected or not.
- 

## Where to Find the Functional Audit

To find the Functional Audit, follow these steps:

- 
- Step 1** Choose a service request, and click on **Details**.
- On the service request details page, the Audit button has two choices:
- Config
  - Functional

**Step 2** Click on **Functional** to display the Functional audit report.

---

## Why a Functional Audit Could Fail

A Functional Audit could fail for the following reasons:

- BGP peering is incorrect
- MPLS setup in the core is faulty
- Remote links are down

A Ping could fail for the following reasons:

- Physical circuit is not setup correctly
- CE is down

## Configuration Audit

A configuration audit verifies if all the commands for a service (service intent) are present on the network elements that participate in the service.

## How to Perform a Configuration Audit

ISC automatically does a config audit whenever a service request is deployed or force-redeployed. You can also create a task to do a configuration audit for one or more service requests.

To create a task to do a configuration audit, follow these steps:

- 
- Step 1** Go to **Monitoring > Tasks > Audit> Config Audit**.
- Step 2** Choose one or more service requests.
- Step 3** Create a schedule for the config-audit task.
- 

## Where to Find the Configuration Audit

After selecting the service request, click on **Details**.

On the details page, the Audit button has two choices:

- Config
- Functional

Click on **Config** to display the Configuration audit report.

## Why a Configuration Audit Could Fail

A configuration audit can fail if some of the commands are removed after provisioning from the network elements. This could happen if the commands are manually removed or they are removed as part of provisioning some other service.

## Editing Configuration Files

To view or edit an existing router configuration file:



### Caution

Exercise caution when editing a configuration file, particularly if you then choose to make the edited file the running configuration file.

**Step 1** Click the **Service Inventory** tab, then go to **Inventory and Connection Manager**.

The Inventory and Connection Manager window is displayed.

**Step 2** Click **Devices**.

The Devices dialog box appears (see Figure 6-61).

**Figure 6-61** *List of Devices Recognized by ISC*

You Are Here: [Service Inventory](#) > [Inventory and Connection Manager](#) > [Devices](#) Customer: None

Devices					
Show Devices with <input type="text" value="Device Name"/> Matching <input <input="" type="button" value="Find"/>					
Showing 1 - 10 of 27 records					
#	<input type="checkbox"/>	Device Name	Management IP Address	Type	Parent Device Name
1.	<input type="checkbox"/>	mlce3	172.29.146.26	Cisco IOS Device	
2.	<input type="checkbox"/>	mlpe1		Cisco IOS Device	
3.	<input type="checkbox"/>	mlpe2		Cisco IOS Device	
4.	<input checked="" type="checkbox"/>	mlpe3	172.29.146.23	Cisco IOS Device	
5.	<input type="checkbox"/>	mlpe4	172.29.146.41	Cisco IOS Device	
6.	<input type="checkbox"/>	mlce4		Cisco IOS Device	
7.	<input type="checkbox"/>	mlsw2	172.29.146.38	Cisco IOS Device	
8.	<input type="checkbox"/>	mlsw1	172.29.146.37	Cisco IOS Device	
9.	<input type="checkbox"/>	mlsw3	172.29.146.39	Cisco IOS Device	
10.	<input type="checkbox"/>	mlsw4	172.29.146.40	Cisco IOS Device	

Rows per page:  Go to page:  of 3

111674

**Step 3** Click the check box next to the device name to choose the configuration file versions you want to view.

**Step 4** Click **Config**.

The Device Configurations dialog box appears (see Figure 6-62).

**Figure 6-62** List of Configurations for the Selected Device

**Device Configurations**

Device: mlpe3 Allowed Configs: unlimited Showing 1 - 2 of 2 records

#	<input type="checkbox"/>	Date	Recyclable
1.	<input type="checkbox"/>	Jan 20 02:10:54 PM PST	Yes
2.	<input type="checkbox"/>	Jan 16 10:36:01 AM PST	Yes

Rows per page: 10 Go to page: 1 of 1

Edit Delete OK

The Device Configurations dialog box displays the list of the current versions of the configuration files for the selected device. The configurations are listed by date and time. The configuration file listed first is the latest version.

- Step 5** Choose the version of the configuration file you want to view, then click **Edit**.  
The contents of the selected configuration file are displayed (see Figure 6-63).

**Figure 6-63** Selected Configuration Displayed

**Device Configuration**

Device: mlpe3 Config: Jan 16 10:36:01 AM PST Recyclable: ☒

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mlpe3
!
boot system disk0:/c7200-p-mz.122-16.6.S
logging snmp-authfail
logging queue-limit 100
enable password moved2nw
!
ip subnet-zero
ip cef
!
!
ip host dirt 171.69.17.19
!
mpls ldp logging neighbor-changes
```

Save Cancel

You can view or edit the displayed device configuration file.

- Step 6** If necessary, edit the configuration file.  
**Step 7** When finished editing the file, click **Save**.



# Provisioning Regular PE-CE Links

This chapter describes how to configure MPLS VPN PE-CE links in the IP Solution Center (ISC) provisioning process. This chapter contains the following major sections:

- MPLS VPN PE-CE Link Overview, page 7-1
- Creating MPLS VPN PE-CE Service Policies, page 7-5
- Creating MPLS VPN PE-CE Service Requests, page 7-14

## MPLS VPN PE-CE Link Overview

This section contains the following sections:

- Network Topology, page 7-2
- Prerequisite Tasks, page 7-2
- Infrastructure Data, page 7-3

To provision an MPLS VPN service in ISC, you must first create an MPLS VPN Service Policy. In ISC, a Service Policy is a set of default configurations for creating and deploying a Service Request.

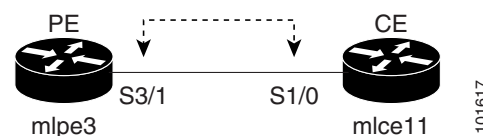
ISC supports two MPLS VPN Service Policy Types: Regular PE-CE and MVRFCE PE-CE. The following scenarios focus on the Regular PE-CE Policy Type.

The Regular PE-CE Policy Type is a normal PE to CE link between two devices. This Policy Type has two options:

- CE Present *enabled* (One PE with one CE; two devices)
- CE Present *disabled* (PE Only with no CE; one device)

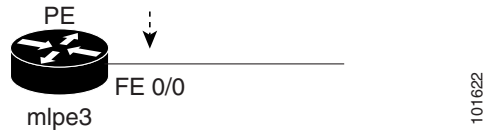
Figure 7-1 shows an example of a normal PE to CE link between two devices.

**Figure 7-1 PE to CE link with CE Present**



In a PE to CE link with CE Present enabled, interfaces S3/1 and S1/0 are configured as an MPLS VPN link in the Service Request process.

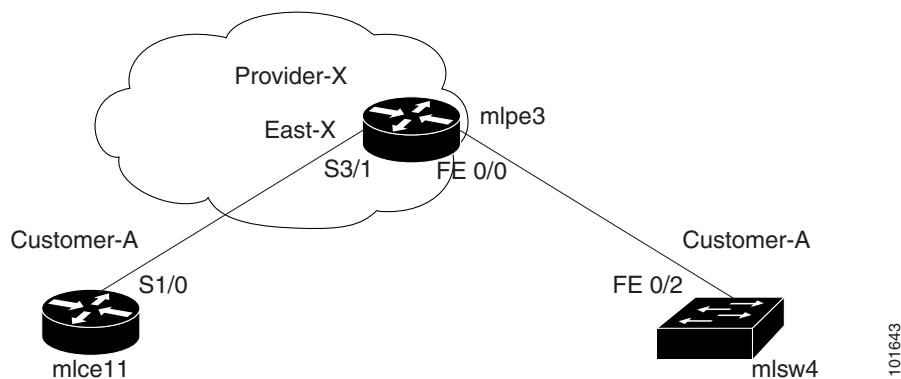
Figure 7-2 shows an example of a PE Only link with no CE.

**Figure 7-2** PE to CE link with No CE

In a PE to CE link with CE Present disabled, interface FE0/0 is configured as an MPLS VPN link in the Service Request process.

## Network Topology

Figure 7-3 shows an overview of the network topology in which the MPLS VPN PE-CE links are created.

**Figure 7-3** Network Topology for MPLS VPN PE-CE Scenarios.

The network topology in Figure 7-3 illustrates the lab environment of a service provider (Provider-X) and one customer (Cust-A). There is one Region (East-X) and one PE (mlpe3.cisco.com). Each customer device (one CE and one CLE) represents a Site (mlce11-Site and mlsw4-Site).

## Prerequisite Tasks

Before you can create a Service Policy in ISC, you must complete the following Inventory Management tasks:

- 
- Step 1** Set up a Customer with a Site.
  - Step 2** Setup a Provider with a Region.
  - Step 3** Import, create, or discover Devices.
  - Step 4** Create CPE and PE.
  - Step 5** Collect Configurations.
  - Step 6** Create Resource Pools and CE routing communities (CERC).
  - Step 7** Define a VPN.
-

## Infrastructure Data

In the subsequent PE-CE scenarios, the following infrastructure data is used:

- Provider: **Provider-X**
- Region: **East-X**
- AS#: **99**
- PE: **mlpe3.cisco.com**
- Device Role: **PE POP**
- Customer: **Cust-A**
- Site: **Cust-A-Site- mlce11**
- CE: **mlce11.cisco.com**
- Device Role: **CPE**
- IP Address Pool:
  - Name: **Provider-X-East-X**
  - Type: **Region**
  - Start: **25.5.0.0**
  - Mask: **30**
  - Size: **16384**
- Route Distinguisher Pool:
  - Name: **99:PROVIDER-X**
  - Start: **50000**
  - Size: **10000**
- Route Target Pool:
  - Name: **99:PROVIDER-X**
  - Start: **50000**
  - Size: **10000**
- VPN
  - Definition: **east-xVPN**
  - *See: Defining a VPN for the PE-CE Link, page 7-3*

## Defining a VPN for the PE-CE Link

During service deployment, ISC generates the Cisco IOS commands to configure the logical VPN relationships.

At the beginning of the provisioning process, before creating a Service Policy, a VPN must be defined within ISC. The first element in a VPN definition is the name of the VPN.

To create a VPN Name, follow these steps:

---

**Step 1** Log in to ISC.

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

The VPN window appears, as shown in Figure 7-4.

**Figure 7-4** VPNs

The screenshot shows the 'VPNs' window within the 'Inventory and Connection Manager' section. The breadcrumb trail is 'You Are Here: > Service Inventory > Inventory and Connection Manager > VPNs'. On the left is a 'TOC' (Table of Contents) menu with options like Service Requests, Inventory Manager, Topology Tool, Devices, Device Groups, Customers, Customer Sites, CPE Devices, Providers, Provider Regions, PE Devices, Access Domains, Resource Pools, CE Routing Communities, VPNs (selected), AAA Servers, Named Physical Circuits, and NPC Rings. The main area is titled 'VPNs' and contains a search bar 'Show VPNs with [VPN Name] matching \*' and a 'Find' button. Below the search bar, it says 'Showing 0 of 0 records'. There is a table header with columns for '#', 'VPN Name', and 'Customer Name'. Below the header, there is a 'Rows per page: 10' dropdown and a pagination control 'Go to page: 1 of 0'. At the bottom right of the table area are 'Create', 'Edit', and 'Delete' buttons.

101619

**Step 3** Click **Create** to create a VPN.

The Create VPN window appears, as shown in Figure 7-5.

**Figure 7-5** Create VPN

The screenshot shows the 'Create VPN' window. The breadcrumb trail is 'You Are Here: > Service Inventory > Inventory and Connection Manager > VPNs'. The left 'TOC' menu is the same as in Figure 7-4. The main area is titled 'Create VPN'. It has two input fields: 'Name \*' with the value 'east-xVPN' and 'Customer \*' with the value 'CUST-A' and a 'Select' button. Below these are the 'MPLS Attributes' section, which includes: 'Create Default CE Routing Community:' with a checked checkbox and a dropdown set to 'PROVIDER-X'; 'Enable Multicast:' with an unchecked checkbox; 'Data MDT Size:' with a dropdown set to '1'; 'Data MDT Threshold:' with a text input '0' and a note '(1 - 4294967)'; and 'CE Routing Communities:' with a large empty box, a 'Select' button, and a 'Remove' button. Below the MPLS attributes is the 'VPLS Attributes' section, which includes: 'Enable VPLS:' with an unchecked checkbox; 'Service Type:' with a dropdown set to 'ERS'; and 'Topology:' with a dropdown set to 'Full Mesh'. At the bottom right are 'Save' and 'Cancel' buttons. A note at the bottom left says 'Note: \* - Required Field'.

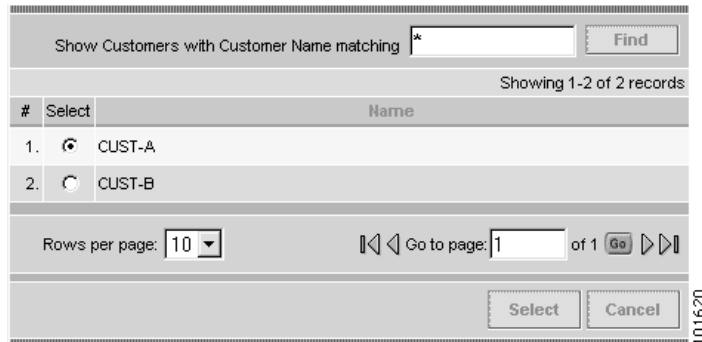
101624

**Step 4** Edit the following attributes:

- **Name:** Enter the *vpn name*. (east-xVPN)
- **Customer:** Click **Select**.

The Select Customer window appears, as shown in Figure 7-6.

**Figure 7-6 Choose Customer**



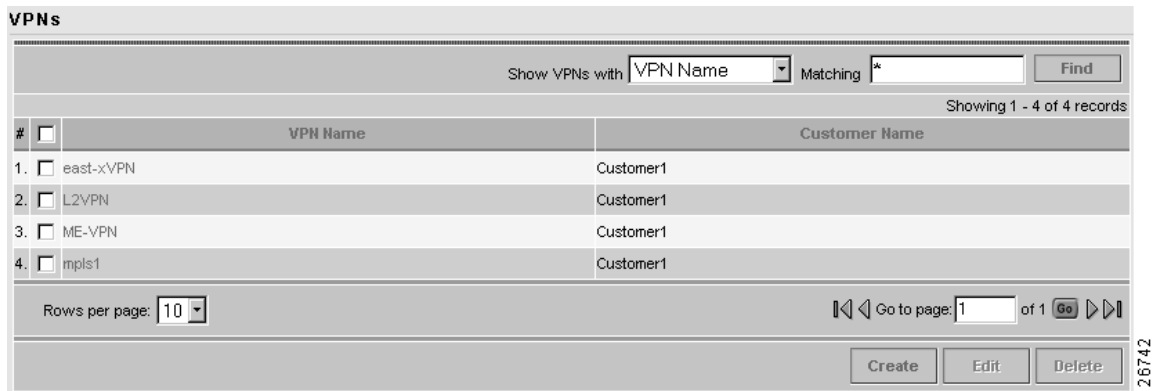
#	Select	Name
1.	<input checked="" type="radio"/>	CUST-A
2.	<input type="radio"/>	CUST-B

**Step 5** Choose a customer and click **Select**.

**Step 6** Click **Save**.

The VPNs window reappears, as shown in Figure 7-7.

**Figure 7-7 VPNs**



#	VPN Name	Customer Name
1.	east-xVPN	Customer1
2.	L2VPN	Customer1
3.	ME-VPN	Customer1
4.	mpls1	Customer1

The VPN Name (**east-xVPN**) is associated with the Customer (**Cust-A**) in this new VPN definition.

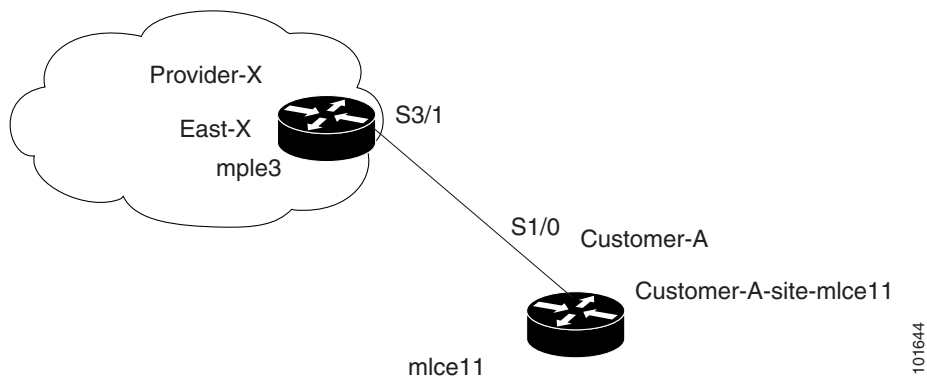
## Creating MPLS VPN PE-CE Service Policies

This section contains the following sections:

- PE-CE Service Policy Overview, page 7-5
- Creating a PE-CE Service Policy, page 7-6
- Creating a PE-NoCE Service Policy, page 7-10

### PE-CE Service Policy Overview

Figure 7-8 shows an example of the PE-CE link that is defined in the PE-CE Service Policy scenario.

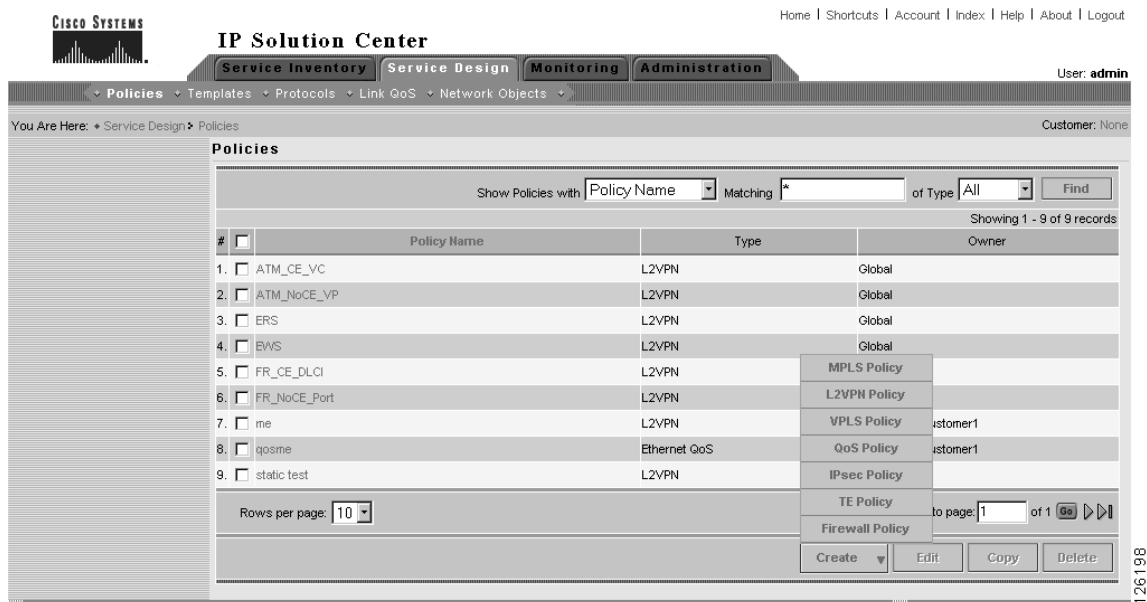
**Figure 7-8 PE-CE Topology**

## Creating a PE-CE Service Policy

To create a PE-CE Service Policy, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Go to **Service Design > Policies**.

The Policies window appears, as shown in Figure 7-9.

**Figure 7-9 Policies**

- Step 3** From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in Figure 7-10.

**Figure 7-10 MPLS Policy Editor - Policy Type**

Attribute	Value
Policy Name *	mpls-pe-ce
Policy Owner:	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
Customer *	Select
Policy Type:	<input checked="" type="radio"/> Regular: PE-CE <input type="radio"/> MVRFCPE: PE-CE
CE Present:	<input checked="" type="checkbox"/>

Note: \* - Required Field

**Step 4** Edit the following attributes:

- **Policy Name:** Enter the *policy name*.
- **Policy Owner:** Choose the Policy Owner.
- **Customer:** See Step 5.
- **Policy Type:** Choose the Policy Type.
- **CE Present:** Choose CE Present.

**Step 5** Click **Select** to specify a Customer.

The Customer for MPLS Policy ownership window appears, as shown in Figure 7-11.

**Figure 7-11 Customer for MPLS Policy**

#	Select	Name
1.	<input checked="" type="radio"/>	CUST-A
2.	<input type="radio"/>	CUST-B

Rows per page: 10 Go to page: 1 of 1 Go Cancel

**Step 6** Choose a customer and click **Select**. (Cust-A)

**Step 7** Click **Next**.

The MPLS Policy Editor - Interface window appears, as shown in Figure 7-12.

**Figure 7-12** The MPLS Policy Editor - Interface

**MPLS Policy Editor - Interface**

Attribute	Value	Editable
<b>Reset all Attribute editable flags:</b>		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Auto-Pick VLAN ID:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Link Speed:	None	<input checked="" type="checkbox"/>
Link Duplex:	None	<input checked="" type="checkbox"/>
ETTH Support:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>CE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

**Step 8** Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - IP Address Scheme window appears, as shown in Figure 7-13.

**Figure 7-13** The MPLS Policy Editor - IP Address Scheme

**MPLS Policy Editor - IP Address Scheme**

Attribute	Value	Editable
<b>PE-CE Interface Addresses/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Extra CE Loopback Required:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

**Step 9** Edit the following attributes:

- **IP Numbering Scheme:** Choose an IP Numbering Scheme.
- **Automatically Assign IP Address:** To have ISC automatically assign IP Addresses, click the check box.
- **IP Address Pool:** Choose the IP Address Pool.

**Step 10** Click **Next**.

The MPLS Policy Editor - Routing Information window appears, as shown in Figure 7-14.

**Figure 7-14 The MPLS Policy Editor - Routing Information**

**MPLS Policy Editor - Routing Information**

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	STATIC	<input checked="" type="checkbox"/>
CsC Support:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

101613

**Step 11** Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - VRF and VPN Membership window appears, as shown in Figure 7-15.

**Figure 7-15 The MPLS Policy Editor - VRF and VPN Membership**

**MPLS Policy Editor - VRF and VPN Membership**

Attribute	Value	Editable
<b>VRF Information</b>		
Export Map:		<input checked="" type="checkbox"/>
Import Map:		<input checked="" type="checkbox"/>
Maximum Routes:	(1-4294967295)	<input checked="" type="checkbox"/>
Maximum Route Threshold:	80 (1-100)	<input checked="" type="checkbox"/>
VRF Description:		<input checked="" type="checkbox"/>
Allocate new route distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Template Association</b>		
Template Enable:	<input type="checkbox"/>	
<b>VPN Selection</b>		
PE VPN Membership:		<input checked="" type="checkbox"/>
Select	Customer	VPN
Provider	CERC	Is Hub
		Add Delete

101614

**Step 12** Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

**Step 13** Click **Finish**.

The Policies window reappears, as shown in Figure 7-16.

**Figure 7-16 Policies**

**Policies**

Show Policies with  matching  of type

Showing 1-1 of 1 records

#	Policy Name	Service	Owner
1.	<input type="checkbox"/> mpls-pe-ce	MPLS	Customer - CUST-A

Rows per page:  Go to page:  of 1

The MPLS VPN PE-CE Service Policy is complete.

## Creating a PE-NoCE Service Policy

To create a PE-NoCE Service Policy, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Go to **Service Design > Policies**.

The Policies window appears, as shown in Figure 7-17.

**Figure 7-17 Policies**

**IP Solution Center**

Home | Shortcuts | Account | Index | Help | About | Logout

User: admin

**Policies** | Templates | Protocols | Link QoS | Network Objects

You Are Here: Service Design > Policies Customer: None

**Policies**

Show Policies with  Matching  of Type

Showing 1 - 9 of 9 records

#	Policy Name	Type	Owner
1.	<input type="checkbox"/> ATM_CE_VC	L2VPN	Global
2.	<input type="checkbox"/> ATM_NoCE_VP	L2VPN	Global
3.	<input type="checkbox"/> ERS	L2VPN	Global
4.	<input type="checkbox"/> EVS	L2VPN	Global
5.	<input type="checkbox"/> FR_CE_DLCl	L2VPN	MPLS Policy
6.	<input type="checkbox"/> FR_NoCE_Port	L2VPN	L2VPN Policy
7.	<input type="checkbox"/> me	L2VPN	VPLS Policy Customer1
8.	<input type="checkbox"/> qosme	Ethernet QoS	QoS Policy Customer1
9.	<input type="checkbox"/> static test	L2VPN	IPsec Policy

Rows per page:  Go to page:  of 1

- Step 3** From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in Figure 7-18.

**Figure 7-18 MPLS Policy Editor - Policy Type**

Attribute	Value
Policy Name*:	impls-pe-noce
Policy Owner:	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
Customer*:	CUST-A <input type="button" value="Select"/>
Policy Type:	<input checked="" type="radio"/> Regular: PE-CE <input type="radio"/> MVRFCPE: PE-CE
CE Present:	<input type="checkbox"/>

Note: \* - Required Field

- Step 4** Edit the following attributes:
- **Policy Name:** Enter the *policy name*.
  - **Policy Owner:** Choose the Policy Owner.
  - **Customer:** See Step 5.
  - **Policy Type:** Choose the Policy Type.
  - **CE Present:** *Do not choose* CE Present.

- Step 5** Click **Select** to specify a Customer.

The Customer for MPLS Policy window appears, as shown in Figure 7-19.

**Figure 7-19 Customer for MPLS Policy**

Customer for MPLS policy ownership

Show Customers with Customer Name matching \*

Showing 1-2 of 2 records

#	Select	Name
1.	<input checked="" type="radio"/>	CUST-A
2.	<input type="radio"/>	CUST-B

Rows per page: 10

- Step 6** Choose a customer and click **Select**.

- Step 7** Click **Next**.

The MPLS Policy Editor - Interface window appears, as shown in Figure 7-20.

**Figure 7-20**      *The MPLS Policy Editor - Interface*

**MPLS Policy Editor - Interface**

Attribute	Value	Editable
<b>Reset all Attribute editable flags:</b>		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Auto-Pick VLAN ID:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Link Speed:	None	<input checked="" type="checkbox"/>
Link Duplex:	None	<input checked="" type="checkbox"/>
ETTH Support:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

101630

**Step 8** Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - IP Address Scheme window appears, as shown in Figure 7-21.

**Figure 7-21**      *The MPLS Policy Editor - IP Address Scheme*

**MPLS Policy Editor - IP Address Scheme**

Attribute	Value	Editable
<b>PE-CE Interface Addresses/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

101633

**Step 9** Edit the following attributes:

- **IP Numbering Scheme:** Choose the IP Numbering Scheme.
- **Automatically Assign IP Address:** To have ISC automatically assign IP Addresses, click the check box.
- **IP Address Pool:** Choose the IP Address Pool.
- Click **Next**.

**Step 10** Click **Next**.

The MPLS Policy Editor - Routing Information window appears, as shown in Figure 7-22.

**Figure 7-22 The MPLS Policy Editor - Routing Information**

**MPLS Policy Editor - Routing Information**

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	STATIC	<input checked="" type="checkbox"/>
CsC Support:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Step 11** Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - VRF and VPN Membership window appears, as shown in Figure 7-23.

**Figure 7-23 The MPLS Policy Editor - VRF and VPN Membership**

**MPLS Policy Editor - VRF and VPN Membership**

Attribute	Value	Editable
<b>VRF Information</b>		
Export Map:		<input checked="" type="checkbox"/>
Import Map:		<input checked="" type="checkbox"/>
Maximum Routes:	(1-4294967295)	<input checked="" type="checkbox"/>
Maximum Route Threshold:	80 (1-100)	<input checked="" type="checkbox"/>
VRF Description:		<input checked="" type="checkbox"/>
Allocate new route distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Template Association</b>		
Template Enable:	<input type="checkbox"/>	
<b>VPN Selection</b>		
PE VPN Membership:		<input checked="" type="checkbox"/>

Select Customer VPN Provider CERC Is Hub

Add Delete

- Step 5 of 5 -

< Back Next > Finish Cancel

**Step 12** Accept the default attributes and choose **Finish**.

The Policies window reappears, as shown in Figure 7-24.

**Figure 7-24 Policies**

**Policies**

Show Policies with  matching  of type

Showing 1-2 of 2 records

#	<input type="checkbox"/>	Policy Name	Service	Owner
1.	<input checked="" type="checkbox"/>	mpls-pe-ce	MPLS	Customer - CUST-A
2.	<input type="checkbox"/>	mpls-pe-noce	MPLS	Customer - CUST-A

Rows per page:   Go to page:  of 1

101641

The MPLS VPN PE-NoCE Service Policy is complete.

## Creating MPLS VPN PE-CE Service Requests

This section contains the following sections:

- Creating a PE-CE Service Request, page 7-14
- Creating a PE-NoCE Service Request, page 7-21

### Creating a PE-CE Service Request

To create a PE-CE Service Request, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.  
The Service Requests window appears, as shown in Figure 7-25.

**Figure 7-25 Service Requests**

**Service Requests**

Show Services with  matching  of type

Showing 1-1 of 1 records

#	<input checked="" type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	<input checked="" type="checkbox"/>	1	DEPLOYED	MPLS	ADD	admin	CUST-A	mpls-pe-ce	10/10/03 4:26 PM	ce2-sw1-sw2-pe2

Rows per page:   Go to page:  of 1

**Auto Refresh:** ☒

101618

- Step 3** From the **Create** drop-down list, choose **MPLS VPN**.  
The Select MPLS Policy window appears, as shown in Figure 7-26.

**Figure 7-26 Choose MPLS Policy**

**Select MPLS Policy**

Show MPLS policies with  matching

Showing 1-5 of 5 records

#	Select	Policy Name	Policy Owner
1.	<input type="radio"/>	mpls-mgmt	Customer - CUST-A
2.	<input type="radio"/>	mpls-mvrfce-pe-ce	Customer - CUST-A
3.	<input type="radio"/>	mpls-mvrfce-pe-noce	Customer - CUST-A
4.	<input checked="" type="radio"/>	mpls-pe-ce	Customer - CUST-A
5.	<input type="radio"/>	mpls-pe-noce	Customer - CUST-A

Rows per page:

101623

**Step 4** Choose the MPLS Policy. (**mpls-pe-ce**)

**Step 5** Click **OK**.

The MPLS Service Request Editor window appears, as shown in Figure 7-27.

**Figure 7-27 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID: \_\_\_\_\_ SR ID: \_\_\_\_\_ SR State: \_\_\_\_\_

Policy: mpls1

Customer: Customer1

Description:

Showing 0 of 0 records

#	<input type="checkbox"/>	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
---	--------------------------	---------	----	--------------	----	--------------	----------------	--------------

Rows per page:

126726

**Step 6** Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in Figure 7-28.

**Figure 7-28 MPLS Service Request Editor - Select CE**

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: POL1

Customer: CUST1

Description:

Showing 1 - 1 of 1 record

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CE		Select PE		Add	N/A

Rows per page: 10

Go to page: 1 of 1

Add Link Delete Link Save Cancel

**Step 7** Click **Select CE**.

The CPE for MPLS VPN Link window appears, as shown in Figure 7-29.

**Figure 7-29 CPE for MPLS VPN Link**

**Select CPE Device - Microsoft Internet Explorer**

Show CPEs with Customer Name Matching \*

Find

Showing 1 - 4 of 4 records

#	Device Name	Customer Name	Site Name	Management Type
1.	mlce7	Customer1	SF	Managed
2.	mlce11	Customer1	NY	Managed
3.	mlce6	Customer1	SF	Managed
4.	mlce10	Customer1	NY	Managed

Rows per page: 10

Go to page: 1 of 1

Select Cancel

**Step 8** Choose the CPE device and click **Select**.

The MPLS Service Request Editor window appears.

**Step 9** Choose the CE Interface from the drop-down box.

The MPLS Service Request Editor window appears.

**Step 10** Click **Select PE**.

The PE for MPLS VPN Link window appears, as shown in Figure 7-30.

**Figure 7-30 PE for MPLS VPN Link**

#	Device Name	Provider Name	Region Name	Role Type
1.	mipe2	Provider1	West	PE_POP
2.	mipe4	Provider1	East	PE_POP
3.	enswostr1	Provider1	West	PE_POP
4.	enswostr2	Provider1	East	PE_POP

**Step 11** Choose the PE device and click **Select**.

The MPLS Service Request Editor window appears.

**Step 12** Choose the PE Interface from the drop-down box.

The MPLS Service Request Editor window appears.

**Step 13** Click **Select PE**.

The PE for MPLS VPN Link window appears, as shown in Figure 7-31.

**Figure 7-31 MPLS Service Request Editor**

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mipe10	FastEthernet0/0	mipe2	Ethernet4/0	Add	N/A

**Step 14** Click **Add** in the Link Attribute cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 7-32.

**Figure 7-32 MPLS Link Attribute Editor - Interface**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>PE Information</b>	
PE	enswosr2
Interface Name:	POS7/1. <input type="text"/>
Interface Description:	<input type="text"/>
Shutdown Interface:	<input checked="" type="checkbox"/>
Encapsulation:	FRAME_RELAY <input type="text"/>
DLCI*:	100 <input type="text"/> (16-1007)
<b>CE Information</b>	
CE	enswosr1
Interface Name:	POS7/1. <input type="text"/>
Interface Description:	<input type="text"/>
Encapsulation:	FRAME_RELAY <input type="text"/>
DLCI*:	100 <input type="text"/> (16-1007)

Note: \* - Required Field

Step 1 of 5 -

< Back Next > Finish Cancel

**PE Information**

**Step 15 Encapsulation:** Choose the PE Encapsulation from the drop-down box.

**Step 16 DLCI:** Enter the *CE DLCI*. (100)

**CE Information**

**Step 17 Encapsulation:** Choose the PE Encapsulation from the drop-down box.

**Step 18 DLCI:** Enter the *PE DLCI*. (100)

**Step 19** Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 7-33.

**Figure 7-33 MPLS Link Attribute Editor - IP Address Scheme**

**MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>PE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered <input type="text"/>
Extra CE Loopback Required:	<input type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool <input type="text"/>

Note: \* - Required Field

**Step 20** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 7-34.

**Figure 7-34 MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	STATIC
CsC Support:	<input type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>
Advertised Routes for CE:	<input type="button" value="Edit"/>
Routes To Reach Other Sites:	<input type="button" value="Edit"/>

Note: \* - Required Field

101645

**Step 21** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears, as shown in Figure 7-35.

**Figure 7-35 MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	<input type="text"/>
Import Map:	<input type="text"/>
Maximum Routes:	<input type="text"/> (1-4294967295)
Maximum Route Threshold *:	<input type="text"/> 80 (1-100)
VRF Description:	<input type="text"/>
Allocate new route distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	
Select	Customer VPN Provider CERC Is Hub
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

Note: \* - Required Field

101646

**Step 22** Click **Add** to join VPN. The Select CERCs window appears as show in Figure 7-36.

**Figure 7-36** *Select CERCs Window*

Customer:  VPN:

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Customer	VPN	Provider	CERC	Topology
1.	<input type="checkbox"/>	Customer1	mpls1	Provider1	cerc1	Hub and Spoke

Rows per page:  Go to page:  of 1

- Step 23** Choose a customer from the drop-down list.
- Step 24** Choose a VPN from the drop-down list.
- Step 25** Choose a VPN from the list.
- Step 26** Click **Join As Hub** or **Join As Spoke**.
- Step 27** Click **Done**. The MPLS Link Attribute Editor - VRF and VPN window reappears, as shown in Figure 7-37.

**Figure 7-37** *MPLS Service Request Editor*

MPLS Policy Editor - VRF and VPN Membership

Attribute	Value	Editable
<b>VRF Information</b>		
Export Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Import Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Maximum Routes:	<input type="text" value="(1-4294967295)"/>	<input checked="" type="checkbox"/>
Maximum Route Threshold:	<input type="text" value="80"/> (1-100)	<input checked="" type="checkbox"/>
VRF Description:	<input type="text"/>	<input checked="" type="checkbox"/>
Allocate New Route Distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VRF And RD Overwrite:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Template Association</b>		
Template Enable:	<input type="checkbox"/>	
<b>VPN Selection</b>		
PE VPN Membership:		<input checked="" type="checkbox"/>

Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	Customer1	mpls1	Provider1	cerc1	<input checked="" type="checkbox"/>

Step 5 of 5 -

- Step 28** Click **Finish**.
- The MPLS Service Request Editor window reappears, as shown in Figure 7-38.

**Figure 7-38 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID: 14      SR ID: 14      SR State: REQUESTED

Policy: mpls1

Customer: Customer1

Description: mpls-pe-ce

Showing 1 - 1 of 1 record

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	25	enswostr1	POS7/1	enswostr2	POS7/2	Edited	N/A

Rows per page: 10      Go to page: 1 of 1

Add Link   Delete Link   Save   Cancel

**Step 29** Enter the Service Request *description* and click **Save**. (**mpls-pe-ce**)

The MPLS Service Requests window reappears, as shown in Figure 7-39.

**Figure 7-39 Service Request**

**Service Requests**

Show Services with Customer Name matching \* of type All Find

Showing 1-2 of 2 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	1	DEPLOYED	MPLS	ADD	admin	CUST-A	mpls-pe-ce	10/10/03 4:26 PM	ce2-sw1-sw2-pe2
2.	2	REQUESTED	MPLS	ADD	admin	CUST-A	mpls-pe-ce	10/12/03 12:46 AM	mpls-pe-ce

Rows per page: 10      Go to page: 1 of 1

Auto Refresh: ☒   Create   Details   Edit   Deploy   Decommission   Purge

The MPLS VPN PE-CE Service Request is in the Requested state and ready to deploy.

## Creating a PE-NoCE Service Request

To create a PE-NoCE Service Request, follow these steps:

**Step 1** Log in to ISC.

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

The Service Requests window appears, as shown in Figure 7-40.

**Figure 7-40 Service Requests**

Service Requests

Show Services with Job ID matching \* of type All Find

Showing 0 of 0 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
---	--------	-------	------	----------------	---------	---------------	-------------	---------------	-------------

Rows per page: 10 Go to page: 1 of 0

Auto Refresh: ☒ Create Details Edit Deploy Decommission Purge

MPLS VPN

- Step 3** From the **Create** drop-down list, choose **MPLS VPN**.  
The Select MPLS Policy window appears, as shown in Figure 7-41.

**Figure 7-41 Select MPLS Policy**

Select MPLS Policy

Show MPLS policies with Policy Name matching \* Find

Showing 1-5 of 5 records

#	Select	Policy Name	Policy Owner
1.	<input type="radio"/>	mpls-mgmt	Customer - CUST-A
2.	<input type="radio"/>	mpls-mvrfce-pe-ce	Customer - CUST-A
3.	<input type="radio"/>	mpls-mvrfce-pe-noce	Customer - CUST-A
4.	<input type="radio"/>	mpls-pe-ce	Customer - CUST-A
5.	<input checked="" type="radio"/>	mpls-pe-noce	Customer - CUST-A

Rows per page: 10 Go to page: 1 of 1

OK Cancel

- Step 4** Choose the MPLS Policy.
- Step 5** Click **OK**.  
The MPLS Service Request Editor window appears, as shown in Figure 7-42.

**Figure 7-42 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: mpls-pe-nocce

Customer: Customer1

Description:

Showing 0 of 0 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
Rows per page: 10								
Go to page: 1 of 1 Go								
<input type="button" value="Add Link"/> <input type="button" value="Delete Link"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>								

**Step 6 Click Add Link.**

The MPLS Service Request Editor window appears, as shown in Figure 7-43.

**Figure 7-43 MPLS Service Request Editor - Select CE**

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: mpls-pe-nocce

Customer: Customer1

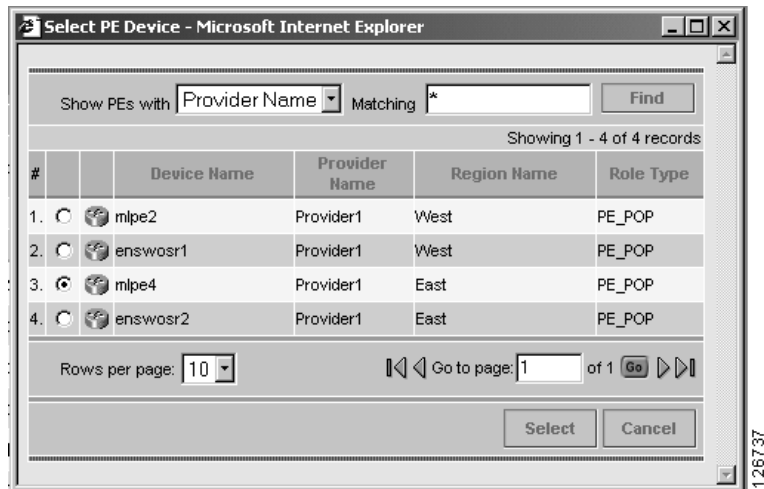
Description:

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="text"/>	Select PE	<input type="text"/>	Add	N/A
Rows per page: 10								
Go to page: 1 of 1 Go								
<input type="button" value="Add Link"/> <input type="button" value="Delete Link"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>								

**Step 7 Click Select PE.**

The PE for MPLS VPN Link window appears, as shown in Figure 7-44.

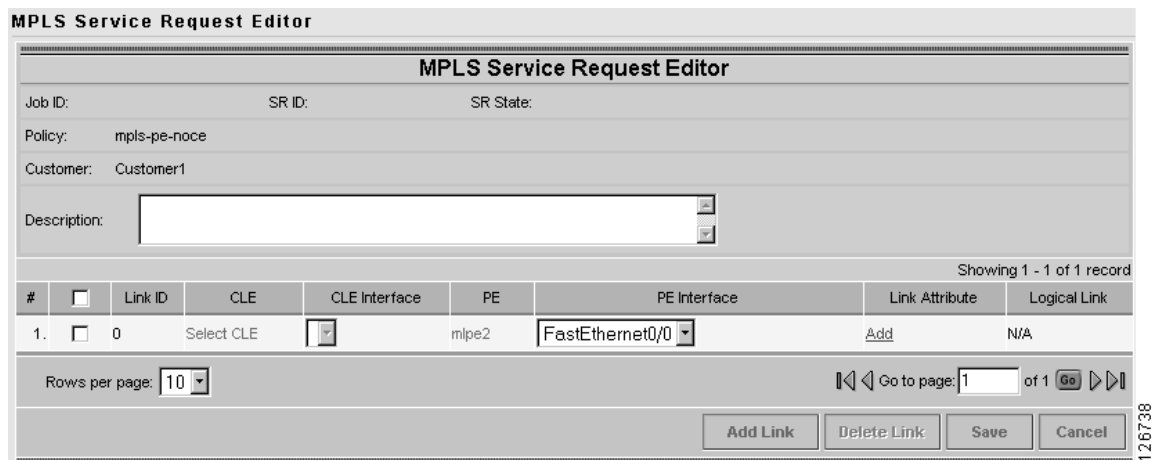
**Figure 7-44** PE for MPLS VPN Link

**Step 8** Choose the PE device and click **Select**.

The MPLS Service Request Editor window appears.

**Step 9** Choose the PE Interface from the drop-down box.

The MPLS Service Request Editor window appears, as shown in Figure 7-45.

**Figure 7-45** MPLS Service Request Editor

**Step 10** Click **Add** in the Link Attribute cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 7-46.

**Figure 7-46 MPLS Link Attribute Editor - Interface**

MPLS Link Attribute Editor - Interface	
Attribute	Value
<b>PE Information</b>	
PE	mlpe2
Interface Name:	FastEthernet0/0. <input type="text"/>
Interface Description:	<input type="text"/>
Shutdown Interface:	<input type="checkbox"/>
CE Encapsulation: ⓘ	DOT1Q ▾
VLAN ID *:	<input type="text"/> (1-4095)
Auto-Pick VLAN ID:	<input type="checkbox"/>
Link Speed:	None ▾
Link Duplex:	None ▾

Note: \* - Required Field

126739

**Step 11** Choose the CE Encapsulation from the drop-down list. (**DOT1Q**)



**Note** This field is needed for deciding PE/UNI encapsulation.

**Step 12** Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 7-47.

**Figure 7-47 MPLS Link Attribute Editor - IP Address Scheme**

MPLS Link Attribute Editor - IP Address Scheme	
Attribute	Value
<b>PE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered ▾
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool ▾

Note: \* - Required Field

101660

**Step 13** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 7-48.

**Figure 7-48 MPLS Link Attribute Editor - Routing Information**

**MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	STATIC
CsC Support:	<input type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>
Advertised Routes for CE:	<input type="button" value="Edit"/>
Routes To Reach Other Sites:	<input type="button" value="Edit"/>

Note: \* - Required Field

101663

**Step 14** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window reappears, as shown in Figure 7-49.

**Figure 7-49 MPLS Link Attribute Editor - VRF and VPN**

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	
Import Map:	
Maximum Routes:	(1-4294967295)
Maximum Route Threshold *:	80 (1-100)
VRF Description:	
Allocate new route distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	
Select	Customer VPN Provider CERC Is Hub
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

Note: \* - Required Field

101646

Click **Add** to join the VPN.

The Join VPN dialog box appears, as shown in Figure 7-50.

**Figure 7-50 MPLS Service Request Editor**

Customer: CUST-A VPN: east-xVPN

Showing 1-1 of 1 records

#	<input checked="" type="checkbox"/>	Customer	VPN	Provider	CERC	Topology
1.	<input checked="" type="checkbox"/>	CUST-A	east-xVPN	PROVIDER-X	Default	Hub and Spoke

Rows per page: 5 Go to page: 1 of 1

Join As Hub Join As Spoke Done

**Step 15** Click the check box to choose the VPN. (**Cust-A east-xVPN**)

**Step 16** Click Join as Hub or Join as Spoke. (**Join as Spoke**)

Click **Done**.

The MPLS Service Request Editor window reappears, as shown in Figure 7-51.

**Figure 7-51 MPLS Service Request Editor**

MPLS Link Attribute Editor - VRF and VPN

Attribute	Value				
<b>VRF Information</b>					
Export Map:					
Import Map:					
Maximum Routes:	(1-4294967295)				
Maximum Route Threshold *:	80 (1-100)				
VRF Description:					
Allocate new route distinguisher:	<input type="checkbox"/>				
VRF And RD Overwrite	<input type="checkbox"/>				
<b>VPN Selection</b>					
PE VPN Membership *:					
Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	CUST-A	east-xVPN	PROVIDER-X	Default	<input type="checkbox"/>
					Add Delete

Note: \* - Required Field

- Step 4 of 4 -

< Back Next > Finish Cancel

**Step 17** Click **Finish**.

The MPLS Service Requests Editor window reappears, as shown in Figure 7-52.

**Figure 7-52 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID:                      SR ID:                      SR State:

Policy: mpls-pe-noce

Customer: Customer1

Description:

Showing 1 - 1 of 1 record

#	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CLE		mlpe2	FastEthernet0/0	Edited	N/A

Rows per page: 10      Go to page: 1 of 1

Add Link   Delete Link   Save   Cancel

**Step 18** Enter the Service Request *description* and click **Save**. (**mpls-pe-noce**)

The MPLS Service Requests window reappears, as shown in Figure 7-53.

**Figure 7-53 Service Request**

You Are Here: Service Inventory > Inventory and Connection Manager > Service Requests      Customer: None

**Service Requests**

Show Services with Job ID Matching \* of Type All Find

Showing 1 - 9 of 9 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	1	DEPLOYED	L2VPN	ADD	SD	Customer1	FR_CE_DLCl	9/22/04 11:20 AM	FR DLCl 51
2.	2	DEPLOYED	L2VPN	MODIFY	SD	Customer1	ATM_CE_VC	9/22/04 11:32 AM	ATM VC 48
3.	4	DEPLOYED	L2VPN	ADD	SD	Customer1	FR_NoCE_Port	9/22/04 11:36 AM	FR port
4.	5	DEPLOYED	L2VPN	ADD	SD	Customer1	ATM_NoCE_VP	9/22/04 11:39 AM	ATM VP
5.	6	REQUESTED	L2VPN	MODIFY	admin	Customer1	ERS	12/1/04 5:34 PM	ERS
6.	8	DEPLOYED	L2VPN	MODIFY	SD	Customer1	EVS	9/28/04 10:11 AM	EVS
7.	13	REQUESTED	QoS	ADD	admin	Customer1	qosme	11/5/04 10:37 AM	
8.	14	REQUESTED	MPLS	ADD	admin	Customer1	mpls1	12/1/04 5:19 PM	
9.	16	REQUESTED	MPLS	ADD	admin	Customer1	mpls-pe-noce	12/2/04 3:12 PM	

Rows per page: 10      Go to page: 1 of 1

Auto Refresh: ☒      Create   Details   Edit   Deploy   Decommission   Purge

Operation: Create MPLS SR  
Status: ☒ Succeeded

The MPLS VPN PE-NoCE Service Request is ready to deploy.



## Provisioning MVRFCE PE-CE Links

---

This chapter describes how to configure MPLS VPN MVRFCE PE-CE links in the IP Solution Center (ISC) provisioning process. This chapter contains the following major sections:

- MPLS VPN MVRFCE PE-CE Link Overview, page 8-1
- Creating MPLS VPN MVRFCE PE-CE Service Policies, page 8-6
- Creating MPLS VPN MVRFCE PE-CE Service Requests, page 8-18

### MPLS VPN MVRFCE PE-CE Link Overview

This section contains the following sections:

- Network Topology, page 8-2
- Prerequisite Tasks, page 8-3
- Infrastructure Data, page 8-3

To provision an MPLS VPN service in ISC, you must first create an MPLS VPN Service Policy. In ISC, a Service Policy is a set of default configurations for creating and deploying a Service Request.

ISC supports two MPLS VPN Service Policy Types: Regular PE-CE and MVRFCE PE-CE. The following scenarios focus on the MVRFCE PE-CE Policy Type.

An MVRFCE PE-CE Policy Type is a PE to CE link with three devices:

- PE
- Multi-VRF CE
- CE

This Policy Type has two options:

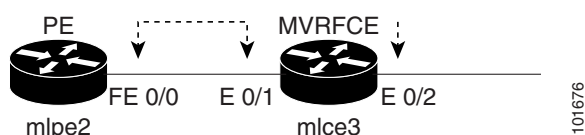
- CE Present *enabled* (One PE with one MVRFCE and one CE; three devices)
- CE Present *disabled* (One PE with one MVRFCE; two devices)

Figure 8-1 shows an example of an MVRFCE PE-CE link with three devices.

**Figure 8-1 MVRFCE PE-CE Link**

In an MVRFCE PE-CE link with CE Present enabled, interfaces FE 0/0, E 0/1, E 0/2 and FE 0/1 are configured as an MPLS VPN link in the Service Request process.

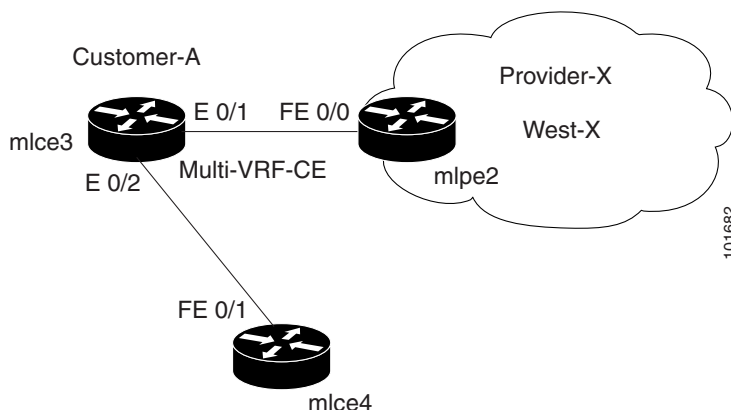
Figure 8-2 shows an example of a PE to MVRFCE link with no CE.

**Figure 8-2 MVRFCE PE-CE Link with No CE**

In an MVRFCE PE-CE link with CE Present disabled, interfaces FE 0/0, E 0/1, and E 0/2 are configured as an MPLS VPN link in the Service Request process.

## Network Topology

Figure 8-3 shows an overview of the network topology in which the MPLS VPN MVRFCE PE-CE links are created.

**Figure 8-3 Network Topology for MPLS VPN MVRFCE PE-CE Scenarios**

The network topology in Figure 8-3 illustrates the lab environment of a service provider (Provider-X) and one customer (Cust-A). There is one Region (West-X) and one PE (mlpe2.cisco.com). Each customer device (one MVRFCE and one CE) represents a Site (mlce3-Site and mlce4-Site).

## Prerequisite Tasks

Before you can create a Service Policy in ISC, you must complete the following Inventory Management tasks:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Set up a Customer with a Site.                           |
| <b>Step 2</b> | Setup a Provider with a Region.                          |
| <b>Step 3</b> | Import, create, or discover Devices.                     |
| <b>Step 4</b> | Create CPE and PE.                                       |
| <b>Step 5</b> | Collect Configurations.                                  |
| <b>Step 6</b> | Create Resource Pools and CE routing communities (CERC). |
| <b>Step 7</b> | Define a VPN.  |
- 

## Infrastructure Data

In the subsequent MVRFCE PE-CE scenarios, the following infrastructure data is used:

- Provider: **Provider-X**
- Region: **West-X**
- AS#: **99**
- PE: **mlpe2.cisco.com**
- Device Role: **PE POP**
- Customer: **Cust-A**
- Site: **Cust-A-Site- mlce3**
- CE: **mlce3.cisco.com**
- Site: **Cust-A-Site- mlce4**
- CE: **mlce4.cisco.com**
- Device Role: **CPE**
- IP Address Pool:
  - Name: **Provider-X-West-X**
  - Type: **Region**
  - Start: **25.7.0.0**
  - Mask: **30**
  - Size: **16384**
- Route Distinguisher Pool:
  - Name: **99:PROVIDER-X**
  - Start: **50000**
  - Size: **10000**

- Route Target Pool:
  - Name: **99:PROVIDER-X**
  - Start: **50000**
  - Size: **10000**
- VPN
  - Definition: **west-xVPN**
  - See: Defining a VPN for the MVRFCE PE-CE Link, page 8-4

## Defining a VPN for the MVRFCE PE-CE Link

During service deployment, ISC generates the Cisco IOS commands to configure the logical VPN relationships.

At the beginning of the provisioning process, before creating a Service Policy, a VPN must be defined within ISC. The first element in a VPN definition is the name of the VPN.

To create a VPN Name, follow these steps:

- 
- Step 1** Log in to ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > VPNs**.  
The VPN window appears, as shown in Figure 8-4.

**Figure 8-4** VPNs

VPNs

Show VPNs with **VPN Name** matching **\*** **Find**

Showing 1-1 of 1 records

#	<input type="checkbox"/>	VPN Name	Customer Name
1.	<input type="checkbox"/>	east-xVPN	CUST-A

Rows per page: **10**

Go to page: **1** of **1** **Go** **Previous** **Next**

**Create** **Edit** **Delete**

- Step 3** Click **Create** to create a VPN.  
The Create VPN window appears, as shown in Figure 8-5.

**Figure 8-5 Create VPN**

You Are Here: > Service Inventory > Inventory and Connection Manager > VPNs

**Create VPN**

Name \*:

Customer \*:

**MPLS Attributes**

Create Default CE Routing Community: ☐

Enable Multicast: ☐

Data MDT Size:

Data MDT Threshold:  (1 - 4294967)

CE Routing Communities:

**VPLS Attributes**

Enable VPLS: ☐

Service Type:

Topology:

Note: \* - Required Field

**Step 4** Edit the following attributes:

- **Name:** Enter the *vpn name*. (**west-xVPN**)
- **Customer:** Click **Select**.

The Select Customer window appears, as shown in Figure 8-6.

**Figure 8-6 Choose Customer**
 CUST-A' and '2. ☐ CUST-B'. At the bottom, there is a 'Rows per page' dropdown set to '10', a 'Go to page:' field with '1' and 'of 1', and 'Go', '<<', '>>', and '>' buttons. At the very bottom are 'Select' and 'Cancel' buttons."/>

Show Customers with Customer Name matching \*

Showing 1-2 of 2 records

#	Select	Name
1.	<input type="radio"/>	CUST-A
2.	<input type="radio"/>	CUST-B

Rows per page:  Go to page:  of 1

**Step 5** Choose a customer and click **Select**.

**Step 6** Click **Next**.

The VPNs window reappears, as shown in Figure 8-7.

**Figure 8-7**      **VPNs**

You Are Here: > Service Inventory > Inventory and Connection Manager > VPNs

**Create VPN**

**TOC**

- Service Requests
- Inventory Manager
- Topology Tool
- Devices
- Device Groups
- Customers
  - Customer Sites
  - CPE Devices
- Providers
  - Provider Regions
  - PE Devices
  - Access Domains
- Resource Pools
- CE Routing Communities
- VPNs**
- AAA Servers
- Named Physical Circuits
- NPC Rings

**MPLS Attributes**

Name\*: west-xVPN

Customer\*: CUST-A Select

Create Default CE Routing Community: ☒ PROVIDER-X

Enable Multicast: ☐

Data MDT Size: 0

Data MDT Threshold: 0 (1 - 4294967)

CE Routing Communities: Select Remove

**VPLS Attributes**

Enable VPLS: ☐

Service Type: ERS

Topology: Full Mesh

Save Cancel

Note: \* - Required Field

101674

The VPN Name (**west-xVPN**) is associated with the Customer (**Cust-A**) in this new VPN definition.

## Creating MPLS VPN MVRFCE PE-CE Service Policies

This section contains the following sections:

- Creating a MVRFCE PE-CE Service Policy, page 8-6
- Creating a PE-NoCE Service Policy, page 8-12

### Creating a MVRFCE PE-CE Service Policy

To create a MVRFCE PE-CE Service Policy, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Go to **Service Design > Policy Manager**.

The Policies window appears, as shown in Figure 8-8.

**Figure 8-8 Policies**

**Policies**

Show Policies with  matching  of type

Showing 1-2 of 2 records

#	<input type="checkbox"/>	Policy Name	Service	Owner
1.	<input type="checkbox"/>	mpls-pe-ce	MPLS	Customer - CUST-A
2.	<input type="checkbox"/>	mpls-pe-noce	MPLS	Customer - CUST-A

Rows per page:

MPLS Policy

**Step 3** From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in Figure 8-9.

**Figure 8-9 MPLS Policy Editor - Policy Type**

**MPLS Policy Editor - Policy Type**

Mode: ADDING

☐ 1. Step 1: Policy Type

☐ 2. ...

Attribute	Value
Policy Name *	mpls-mvrfce-pe-ce
Policy Owner:	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
Customer *	<input type="button" value="Select"/>
Policy Type:	<input type="radio"/> Regular: PE-CE <input checked="" type="radio"/> MVRFCE: PE-CE
CE Present:	<input checked="" type="checkbox"/>

Note: \* - Required Field

**Step 4** Edit the following attributes:

- **Policy Name:** Enter the *policy name*.
- **Policy Owner:** Choose the Policy Owner.
- **Customer:** See Step 5.
- **Policy Type:** Choose the Policy Type. (**Regular MVRFCE PE-CE**)
- **CE Present:** Choose CE Present. (**CE Present**)

**Step 5** Click **Select** to specify a Customer.

The Customer for MPLS Policy ownership window appears, as shown in Figure 8-10.

Figure 8-10 Customer for MPLS Policy

Customer for **MPLS** policy ownership

Show Customers with Customer Name matching \*  Find

Showing 1-2 of 2 records

#	Select	Name
1.	<input checked="" type="radio"/>	CUST-A
2.	<input type="radio"/>	CUST-B

Rows per page: 10 Go to page: 1 of 1

Select Cancel

**Step 6** Choose a Customer and click **Select**. (Cust-A)

**Step 7** Click **Next**.

The MPLS Policy Editor - PE Interface window appears, as shown in Figure 8-11.

Figure 8-11 The MPLS Policy Editor - PE Interface

MPLS Policy Editor - Interface

Attribute	Value	Editable
Reset all Attribute editable flags:		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>MVRFCE PE Facing Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

**Step 8** Click **Next**.

The MPLS Policy Editor - Interface window appears, as shown in Figure 8-11.

**Figure 8-12**      *The MPLS Policy Editor - CE Interface*

MPLS Policy Editor - Interface		
Attribute	Value	Editable
<b>MVRFCE CE Facing Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
<b>CE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

101677

**Step 9** Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - IP Address Scheme window appears, as shown in Figure 8-13.

**Figure 8-13**      *The MPLS Policy Editor - IP Address Scheme*

MPLS Policy Editor - IP Address Scheme		
Attribute	Value	Editable
<b>PE-MVRFCE Interface Address/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

101678

The MPLS Policy Editor - IP Address Scheme window appears, as shown in Figure 8-13.

**Figure 8-14**      *The MPLS Policy Editor - IP Address Scheme*

MPLS Policy Editor - IP Address Scheme		
Attribute	Value	Editable
<b>MVRFCE-CE Interface Addresses/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Extra CE Loopback Required:	<input type="checkbox"/>	<input type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

101679

**Step 10** Edit the following attributes:

- **IP Numbering Scheme:** Choose an IP Numbering Scheme.
- **Automatically Assign IP Address:** To have ISC automatically assign IP Addresses, click the check box.

- **IP Address Pool:** Choose the IP Address Pool.

**Step 11** Click **Next**.

The MPLS Policy Editor - Routing Information window appears, as shown in Figure 8-15.

**Figure 8-15** The MPLS Policy Editor - Routing Information

Attribute	Value	Editable
<b>PE-MVRFCE Routing Information</b>		
Routing Protocol	STATIC	<input checked="" type="checkbox"/>
Give Only Default Routes to MVRFCE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Step 12** Click **Next** to accept the defaults.

The MPLS Policy Editor - Routing Information window appears, as shown in Figure 8-16.

**Figure 8-16** The MPLS Policy Editor - Routing Information

MPLS Policy Editor - Routing Information		
Attribute	Value	Editable
<b>MVRFCE-CE Routing Information</b>		
Routing Protocol	STATIC	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Step 13** Click **Next** to accept the defaults.



**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - VRF and VPN Membership window appears, as shown in Figure 8-17.

**Figure 8-17 The MPLS Policy Editor - VRF and VPN Membership**

**MPLS Policy Editor - VRF and VPN Membership**

Attribute	Value	Editable
<b>VRF Information</b>		
Export Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Import Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Maximum Routes:	<input type="text"/> (1-4294967295)	<input checked="" type="checkbox"/>
Maximum Route Threshold:	<input type="text"/> 80 (1-100)	<input checked="" type="checkbox"/>
VRF Description:	<input type="text"/>	<input checked="" type="checkbox"/>
Allocate new route distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Template Association</b>		
Template Enable:	<input type="checkbox"/>	
<b>VPN Selection</b>		
PE VPN Membership:		<input checked="" type="checkbox"/>

Select Customer VPN Provider CERC Is Hub

Add Delete

- Step 8 of 8 -

< Back Next > Finish Cancel

**Step 14** Click **Next** to accept the defaults.



**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

**Step 15** Click **Finish**.

The Policies window reappears, as shown in Figure 8-18.

**Figure 8-18 Policies**

**Policies**

Show Policies with  matching  of type  Find

Showing 1-1 of 1 records

#	Policy Name	Service	Owner
1.	<input type="checkbox"/> mpls-mvrfce-pe-ce	MPLS	Customer - CUST-A

Rows per page:  Go to page:  of 1

Create Edit Delete

The MPLS VPN MVRFCE PE-CE Service Policy is complete.

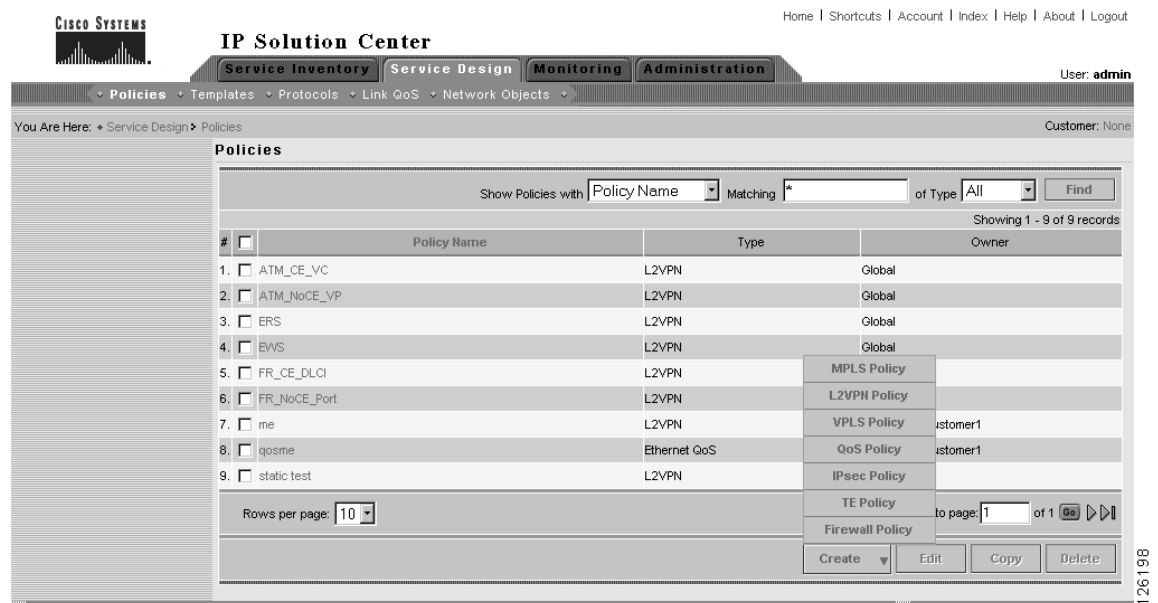
## Creating a PE-NoCE Service Policy

To create a PE-NoCE Service Policy, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Go to **Service Design > Policy Manager**.

The Policies window appears, as shown in Figure 8-19.

**Figure 8-19 Policies**



- Step 3** From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in Figure 8-20.

**Figure 8-20 MPLS Policy Editor - Policy Type**

**MPLS Policy Editor - Policy Type**

Attribute	Value
<b>Policy Name *</b>	mpls-mvrfce-pe-noce
<b>Policy Owner:</b>	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
<b>Customer *</b>	CUST-A <input type="button" value="Select"/>
<b>Policy Type:</b>	<input type="radio"/> Regular: PE-CE <input checked="" type="radio"/> MVRFCE: PE-CE
<b>CE Present:</b>	<input type="checkbox"/>

Note: \* - Required Field

**Step 4** Edit the following attributes:

- **Policy Name:** Enter the *policy name*.
- **Policy Owner:** Choose the Policy Owner.
- **Customer:** See Step 5.
- **Policy Type:** Choose the Policy Type. (MVRFCE PE-CE)
- **CE Present:** *Do not choose* CE Present.

**Step 5** Click **Select** to specify a Customer.

The Customer for MPLS Policy window appears, as shown in Figure 8-21.

**Figure 8-21 Customer for MPLS Policy**

Customer for MPLS policy ownership

Show Customers with Customer Name matching  Find

Showing 1-2 of 2 records

#	Select	Name
1.	<input checked="" type="radio"/>	CUST-A
2.	<input type="radio"/>	CUST-B

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

**Step 6** Choose a customer and click **Select**.

**Step 7** Click **Next**.

The MPLS Policy Editor - Interface window appears, as shown in Figure 8-22.

**Figure 8-22 The MPLS Policy Editor - PE Interface**

MPLS Policy Editor - Interface

Attribute	Value	Editable
<b>Reset all Attribute editable flags:</b>		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>MVRFCE PE Facing Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

The MPLS Policy Editor - Interface window appears, as shown in Figure 8-23.

**Step 8** Click **Next** to accept the defaults.

**Figure 8-23** The MPLS Policy Editor - CE Interface

MPLS Policy Editor - Interface		
Attribute	Value	Editable
<b>MVRFCE CE Facing Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

**Step 9** Click **Next** to accept the defaults.



**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - IP Address Scheme window appears, as shown in Figure 8-24.

**Figure 8-24** The MPLS Policy Editor - IP Address Scheme

MPLS Policy Editor - IP Address Scheme		
Attribute	Value	Editable
<b>PE-MVRFCE Interface Address/Mask</b>		
IP Numbering Scheme:	IP Numbered	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool	<input checked="" type="checkbox"/>

**Step 10** Edit the following attributes:

- **IP Numbering Scheme:** Choose the IP Numbering Scheme.
- **Automatically Assign IP Address:** To have ISC automatically assign IP Addresses, click the check box.
- **IP Address Pool:** Choose the IP Address Pool.
- Click **Next**.

**Step 11** Click **Next**.

The MPLS Policy Editor - IP Address Scheme window appears, as shown in Figure 8-25.

**Figure 8-25 The MPLS Policy Editor - IP Address Scheme**

MPLS Policy Editor - IP Address Scheme		
Attribute	Value	Editable
<b>MVRFCE-CE Interface Addresses/Mask</b>		
IP Numbering Scheme:	IP Numbered ▾	<input checked="" type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool ▾	<input checked="" type="checkbox"/>

101709

**Step 12** Edit the following attributes:

- **IP Numbering Scheme:** Choose the IP Numbering Scheme.
- **Automatically Assign IP Address:** To have ISC automatically assign IP Addresses, click the check box.
- **IP Address Pool:** Choose the IP Address Pool.

Click **Next**.

The MPLS Policy Editor - Routing Information window appears, as shown in Figure 8-26.

**Figure 8-26 The MPLS Policy Editor - Routing Information**

MPLS Policy Editor - Routing Information		
Attribute	Value	Editable
<b>PE-MVRFCE Routing Information</b>		
Routing Protocol	STATIC ▾	<input checked="" type="checkbox"/>
Give Only Default Routes to MVRFCE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>

101710

**Step 13** Click **Next** to accept the defaults.

The MPLS Policy Editor - Routing Information window appears, as shown in Figure 8-27.

**Figure 8-27 The MPLS Policy Editor - Routing Information**

MPLS Policy Editor - Routing Information		
Attribute	Value	Editable
<b>MVRFCE-CE Routing Information</b>		
Routing Protocol	STATIC ▾	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

101714

Click **Next** to accept the defaults.

**Note**

Make sure the Editable check boxes are checked, so you can edit these attributes in the Service Request process.

The MPLS Policy Editor - VRF and VPN Membership window appears, as shown in Figure 8-28.

### MPLS Policy Editor - VRF and VPN Membership

Attribute	Value	Editable
<b>VRF Information</b>		
Export Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Import Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Maximum Routes:	<input type="text"/> (1-4294967295)	<input checked="" type="checkbox"/>
Maximum Route Threshold:	<input type="text"/> 80 (1-100)	<input checked="" type="checkbox"/>
VRF Description:	<input type="text"/>	<input checked="" type="checkbox"/>
Allocate new route distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Template Association</b>		
Template Enable:	<input type="checkbox"/>	
<b>VPN Selection</b>		
PE VPN Membership:		<input checked="" type="checkbox"/>

Select	Customer	VPN	Provider	CERC	Is Hub
--------	----------	-----	----------	------	--------

**Figure 8-29**      **VPN Dialog Box**

Customer:  VPN:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Customer	VPN	Provider	CERC	Topology
1.	<input type="checkbox"/>	CUST-A	west-xVPN	PROVIDER-X	Default	Hub and Spoke

Rows per page:    Go to page:  of 1

**Figure 8-30 The MPLS Policy Editor - VRF and VPN Membership**

**MPLS Policy Editor - VRF and VPN Membership**

Attribute	Value	Editable
<b>VRF Information</b>		
Export Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Import Map:	<input type="text"/>	<input checked="" type="checkbox"/>
Maximum Routes:	<input type="text"/> (1-4294967295)	<input checked="" type="checkbox"/>
Maximum Route Threshold:	<input type="text"/> 80 (1-100)	<input checked="" type="checkbox"/>
VRF Description:	<input type="text"/>	<input checked="" type="checkbox"/>
Allocate new route distinguisher:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Template Association</b>		
Template Enable:	<input type="checkbox"/>	
<b>VPN Selection</b>		
PE VPN Membership:		<input checked="" type="checkbox"/>

Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	CUST-A	west-x-VPN	PROVIDER-X	Default	<input checked="" type="checkbox"/>

Add Delete

- Step 8 of 8 -

< Back Next > Finish Cancel

Click **Finish**.

The Policies window reappears, as shown in Figure 8-31.

**Figure 8-31 Policies**

**CISCO SYSTEMS** **IP Solution Center**

Home | Shortcuts | Account | Index | Help | About | Logout

User: admin

Service Inventory Service Design **Monitoring** Administration

Polices Templates Protocols Link QoS Network Objects

You Are Here: Service Design Polices Customer: None

**Policies**

Show Policies with Policy Name Matching \* of Type All Find

Showing 1 - 9 of 9 records

#	Policy Name	Type	Owner
1.	<input type="checkbox"/> ATM_CE_VC	L2VPN	Global
2.	<input type="checkbox"/> ATM_NoCE_VP	L2VPN	Global
3.	<input type="checkbox"/> ERS	L2VPN	Global
4.	<input type="checkbox"/> BWS	L2VPN	Global
5.	<input type="checkbox"/> FR_CE_DLCl	L2VPN	MPLS Policy
6.	<input type="checkbox"/> FR_NoCE_Port	L2VPN	L2VPN Policy
7.	<input type="checkbox"/> me	L2VPN	VPLS Policy customer1
8.	<input type="checkbox"/> qosme	Ethernet QoS	QoS Policy customer1
9.	<input type="checkbox"/> static test	L2VPN	IPsec Policy

Rows per page: 10

TE Policy to page: 1 of 1

Firewall Policy

Create Edit Copy Delete

The MPLS VPN PE-NoCE Service Policy is complete.

## Creating MPLS VPN MVRFCE PE-CE Service Requests

This section contains the following sections:

- Creating a MVRFCE PE-CE Service Request, page 8-18
- Creating a MVRFCE PE-NoCE Service Request, page 8-27

### Creating a MVRFCE PE-CE Service Request

To create a MVRFCE PE-CE Service Request, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears, as shown in Figure 8-32.

**Figure 8-32** Service Requests

- Step 3** From the **Create** drop-down list, choose **MPLS Policy**.
- The Select MPLS Policy window appears, as shown in Figure 8-33.

**Figure 8-33**      **Select MPLS Policy**

**Select MPLS Policy**

Show MPLS policies with  matching

Showing 1-5 of 5 records

#	Select	Policy Name	Policy Owner
1.	<input type="radio"/>	mpls-mgmt	Customer - CUST-A
2.	<input checked="" type="radio"/>	mpls-mvrfce-pe-ce	Customer - CUST-A
3.	<input type="radio"/>	mpls-mvrfce-pe-noce	Customer - CUST-A
4.	<input type="radio"/>	mpls-pe-ce	Customer - CUST-A
5.	<input type="radio"/>	mpls-pe-noce	Customer - CUST-A

Rows per page:       Go to page:  of 1

101701

**Step 4** Choose the MPLS Policy. (**mpls-mvrfce-pe-ce**)

**Step 5** Click **OK**.

The MPLS Service Request Editor window appears, as shown in Figure 8-34.

**Figure 8-34**      **MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID:      SR ID:      SR State:

Policy: mpls-mvrfce-pe-ce

Description:

Showing 0 of 0 records

#	<input type="checkbox"/>	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
---	--------------------------	---------	----	--------------	----------------------------	--------	----------------------------	----	--------------	----------------	--------------

Rows per page:       Go to page:  of 0

101702

**Step 6** Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in Figure 8-35.

**Figure 8-35** *MPLS Service Request Editor - Select CE*

**MPLS Service Request Editor**

Job ID:                      SR ID:                      SR State:

Policy: mpls-mvrfce-pe-ce

Description:

Showing 1-1 of 1 records

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CE			Select MVRFCE		Select PE		Add	N/A

Rows per page: 10      Go to page: 1 of 1

Add Link   Delete Link   Save   Cancel

101705

**Step 7** Click **Select CE**.

The CPE for MPLS VPN Link window appears, as shown in Figure 8-36.

**Figure 8-36** *CPE for MPLS VPN Link*

**CPE for MPLS VPN Link**

Show CPEs with Customer Name matching \*  Find

Showing 1-10 of 15 records

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	<input type="radio"/>	mlce10.cisco.com	CUST-A	CUST-A-Site-mlce10	MANAGED
2.	<input type="radio"/>	mlce11.cisco.com	CUST-A	CUST-A-Site-mlce11	MANAGED
3.	<input checked="" type="radio"/>	mlce4.cisco.com	CUST-A	CUST-A-Site-mlce4	MANAGED
4.	<input type="radio"/>	mlce5.cisco.com	CUST-A	CUST-A-Site-mlce5	MANAGED
5.	<input type="radio"/>	mlce6.cisco.com	CUST-A	CUST-A-Site-mlce6	MANAGED
6.	<input type="radio"/>	mlce7.cisco.com	CUST-A	CUST-A-Site-mlce7	MANAGED
7.	<input type="radio"/>	mlce1.cisco.com	CUST-B	CUST-B-Site-mlce1	MANAGED
8.	<input type="radio"/>	mlce12.cisco.com	CUST-B	CUST-B-Site-mlce12	MANAGED
9.	<input type="radio"/>	mlce13.cisco.com	CUST-B	CUST-B-Site-mlce13	MANAGED
10.	<input type="radio"/>	mlce14.cisco.com	CUST-B	CUST-B-Site-mlce14	MANAGED

Rows per page: 10      Go to page: 1 of 2

Select   Cancel

101706

**Step 8** Choose the CPE Device and click **Select**.

The MPLS Service Request Editor window appears, as shown in Figure 8-37.

**Figure 8-37 MPLS Service Request Editor - Select MVRFCE**

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce4	FastEthernet0/1		Select MVRFCE		Select PE		Add	N/A

**Step 9** Choose the CE Interface from the drop-down box.

**Step 10** Click **Select MVRFCE**.

The MVRFCE for MPLS VPN Link window appears, as shown in Figure 8-38.

**Figure 8-38 PE for MPLS VPN Link**

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	<input checked="" type="radio"/>	mlce3.cisco.com	CUST-A	CUST-A-Site-mlce3	MULTI_VRF

**Step 11** Choose the MVRFCE and click **Select**.

The MPLS Service Request Editor window appears, as shown in Figure 8-39.

**Figure 8-39 MPLS Service Request Editor - Select MVRFCE CE Facing Interface**

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Select One	Select PE		Add	N/A

**Step 12** Choose the MVRFCE CE Facing Interface from the drop-down box.

**Step 13** Choose the MVRFCE PE Facing Interface from the drop-down box.

The MPLS Service Request Editor window appears, as shown in Figure 8-40.

**Figure 8-40 PE for MPLS VPN Link**

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: mpls-mvrfce-pe-ce

Description:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Add	Details...

**Step 14** Click **Add** in the Link Attribute cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 8-41.

**Figure 8-41 MPLS Link Attribute Editor - Interface**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>PE Information</b>	
PE	mlpe2
Interface Name:	FastEthernet0/0.
Interface Description:	
Shutdown Interface:	<input type="checkbox"/>
Encapsulation:	DOT1Q
VLAN ID *:	510 (1-4095)
<b>MVRFCE PE Facing Information</b>	
MVRFCE	mlce3
Interface Name:	Ethernet0/1.
Interface Description:	
Encapsulation:	DOT1Q

Note: \* - Required Field

- Step 1 of 7 -

< Back Next > Finish Cancel

#### PE Information

**Step 15 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

**Step 16 VLAN ID:** Enter the *PE VLAN ID*. (**510**)

#### MVRFCE PE Facing Information

**Step 17 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

**Step 18** Click **Next**.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 8-42.

**Figure 8-42 MPLS Link Attribute Editor - Interface**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>MVRFCE CE Facing Information</b>	
<b>MVRFCE</b>	mice3
Interface Name:	Ethernet0/2. <input type="text"/>
Interface Description:	<input type="text"/>
Encapsulation:	DOT1Q <input type="text"/>
VLAN ID *:	530 (1-4095)
<b>CE Information</b>	
<b>CE</b>	mice4
Interface Name:	FastEthernet0/1. <input type="text"/>
Interface Description:	<input type="text"/>
Encapsulation:	DOT1Q <input type="text"/>

Note: \* - Required Field

- Step 2 of 7 -

< Back Next > Finish Cancel

**MVRFCE CE Information**

**Step 19 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

**Step 20 VLAN ID:** Enter the *PE VLAN ID*. (**530**)

**MVRFCE PE Facing Information**

**Step 21 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 8-43.

**Figure 8-43 MPLS Link Attribute Editor - IP Address Scheme**

**MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>PE-MVRFCE Interface Address/Mask</b>	
IP Numbering Scheme:	IP Numbered <input type="text"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool <input type="text"/>

Note: \* - Required Field

**Step 22** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 8-44.

**Figure 8-44 MPLS Link Attribute Editor - IP Address Scheme**

**MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>MVRFCE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered ▾
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool ▾

Note: \* - Required Field

101689

Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 8-45.

**Figure 8-45 MPLS Link Attribute Editor - Routing Information**

**MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>PE-MVRFCE Routing Information</b>	
Routing Protocol	STATIC ▾
Give Only Default Routes to MVRFCE:	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>
Advertised Routes for MVRFCE:	Edit
Routes To Reach Other Sites:	Edit

Note: \* - Required Field

101690

**Step 23** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 8-46.

**Figure 8-46 MPLS Link Attribute Editor - Routing Information**

**MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>MVRFCE-CE Routing Information</b>	
Routing Protocol	STATIC ▾
Give Only Default Routes to CE:	<input type="checkbox"/>
Advertised Routes for CE:	Edit
Routes To Reach Other Sites:	Edit

Note: \* - Required Field

101691

Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears, as shown in Figure 8-47.

**Figure 8-47 MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	
Import Map:	
Maximum Routes:	(1-4294967295)
Maximum Route Threshold *:	80 (1-100)
VRF Description:	
Allocate new route distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	

Select	Customer	VPN	Provider	CERC	Is Hub
--------	----------	-----	----------	------	--------

Note: \* - Required Field

- Step 7 of 7 -

< Back Next > Finish Cancel

**Step 24** Click **Add** to join VPN.

The MPLS Link Attribute Editor - VRF and VPN window appears, as shown in Figure 8-48.

**Figure 8-48 MPLS Link Attribute Editor - VRF and VPN**

Customer: CUST-A VPN: west-xVPN

Showing 1-1 of 1 records

#		Customer	VPN	Provider	CERC	Topology
1.	<input type="checkbox"/>	CUST-A	west-xVPN	PROVIDER-X	Default	Hub and Spoke

Rows per page: 5 Go to page: 1 of 1 Go

Join As Hub Join As Spoke Done

Click **Add** to join VPN.

The MPLS Link Attribute Editor - VRF and VPN window reappears, as shown in Figure 8-49.

**Figure 8-49 MPLS Service Request Editor**

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value				
<b>VRF Information</b>					
Export Map:	<input type="text"/>				
Import Map:	<input type="text"/>				
Maximum Routes:	<input type="text"/> (1-4294967295)				
Maximum Route Threshold *:	<input type="text"/> 80 (1-100)				
VRF Description:	<input type="text"/>				
Allocate new route distinguisher:	<input type="checkbox"/>				
VRF And RD Overwrite	<input type="checkbox"/>				
<b>VPN Selection</b>					
PE VPN Membership *:					
Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	CUST-A	west-xVPN	PROVIDER-X	Default	<input checked="" type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/>					

Note: \* - Required Field

- Step 7 of 7 -

**Step 25** Click **Finish**.

The MPLS Service Request Editor window reappears, as shown in Figure 8-50.

**Figure 8-50 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID: 7      SR ID: 8      SR State: REQUESTED

Policy: mpls-mvrfce-pe-ce

Description:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CE	CE Interface	MVRFC CE Facing Interface	MVRFC	MVRFC PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	6	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Edited	Details...

Rows per page:       Go to page:  of 1

**Step 26** Enter the Service Request *description* and click **Save**. (mpls-mvrfce-pe-ce)

The MPLS Service Requests window reappears, as shown in Figure 8-51.

**Figure 8-51 Service Request**

**Service Requests**

Show Services with  matching  of type

Showing 1-4 of 4 records

#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	<input type="checkbox"/>	1	DEPLOYED	MPLS	ADD	admin	CUST-A	mpls-pe-ce	10/10/03 4:26 PM	ce2-sw1-sw2-pe2
2.	<input type="checkbox"/>	2	REQUESTED	MPLS	ADD	admin	CUST-A	mpls-pe-ce	10/12/03 12:46 AM	mpls-pe-ce
3.	<input type="checkbox"/>	6	REQUESTED	MPLS	ADD	admin	CUST-A	mpls-pe-noce	10/12/03 9:06 PM	mpls-pe-noce
4.	<input type="checkbox"/>	7	REQUESTED	MPLS	ADD	admin	CUST-A	mpls-mvrfce-pe-ce	10/14/03 1:57 PM	

Rows per page:

Auto Refresh: ☒

**MPLS VPN**

The MPLS VPN MVRFCE PE-CE Service Request is in the Requested state and ready to deploy.

## Creating a MVRFCE PE-NoCE Service Request

To create a MVRFCE PE-NoCE Service Request, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.  
The Service Requests window appears, as shown in Figure 8-52.

**Figure 8-52 Service Requests**

**Service Requests**

Show Services with  matching  of type

Showing 0 of 0 records

#	<input checked="" type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
---	-------------------------------------	--------	-------	------	----------------	---------	---------------	-------------	---------------	-------------

Rows per page:

Auto Refresh: ☒

**MPLS VPN**

- Step 3** From the **Create** drop-down list, choose **MPLS VPN**.  
The Select MPLS Policy window appears, as shown in Figure 8-53.

**Figure 8-53** *Select MPLS Policy*

**Select MPLS Policy**

Show MPLS policies with  matching

Showing 1-5 of 5 records

#	Select	Policy Name	Policy Owner
1.	<input type="radio"/>	mpls-mgmt	Customer - CUST-A
2.	<input type="radio"/>	mpls-mvrfce-pe-ce	Customer - CUST-A
3.	<input checked="" type="radio"/>	mpls-mvrfce-pe-noce	Customer - CUST-A
4.	<input type="radio"/>	mpls-pe-ce	Customer - CUST-A
5.	<input type="radio"/>	mpls-pe-noce	Customer - CUST-A

Rows per page:

**Step 4** Choose the MPLS Policy. (**mpls-mvrfce-pe-noce**)

**Step 5** Click **OK**.

The MPLS Service Request Editor window appears, as shown in Figure 8-54.

**Figure 8-54** *MPLS Service Request Editor*

**MPLS Service Request Editor**

Job ID: \_\_\_\_\_ SR ID: \_\_\_\_\_ SR State: \_\_\_\_\_

Policy: mpls-mvrfce-pe-noce

Description:

Showing 0 of 0 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
---	--------------------------	---------	-----	---------------	----------------------------	--------	----------------------------	----	--------------	----------------	--------------

Rows per page:

**Step 6** Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in Figure 8-55.

**Figure 8-55 MPLS Service Request Editor - Select MVRFCE**

**MPLS Service Request Editor**

Job ID:                      SR ID:                      SR State:

Policy:    mpl-mvrfce-pe-noc

Description:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="button" value="v"/>	<input type="button" value="v"/>	Select MVRFCE	<input type="button" value="v"/>	Select PE	<input type="button" value="v"/>	Add	N/A

Rows per page:       Go to page:  of 1

101726

**Step 7** Click **Select MVRFCE**.

The CPE for MPLS VPN Link window appears, as shown in Figure 8-56.

**Figure 8-56 CPE for MPLS VPN Link**

**CPE for MPLS VPN Link**

Show CPEs with  matching

Showing 1-1 of 1 records

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	<input checked="" type="radio"/>	mlce3.cisco.com	CUST-A	CUST-A-Site-mlce3	MULTI_VRF

Rows per page:       Go to page:  of 1

101727

**Step 8** Choose the MVRFCE and click **Select**.

The MPLS Service Request Editor window appears, as shown in Figure 8-57.

**Step 9** Click **Select MVRFCE**.

**Figure 8-57 MPLS Service Request Editor - MVRFCE CE Facing Interface**

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: mpls-mvrfce-pe-noc

Description:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="text"/>	Select One	mlce3	Select One	Select PE	<input type="text"/>	Add	N/A

Rows per page: 10 Go to page: 1 of 1

Add Link Delete Link Save Cancel

**Step 10** Choose the MVRFCE CE Facing Interface from the drop-down box.

**Step 11** Choose the MVRFCE PE Facing Interface from the drop-down box.

The MPLS Service Request Editor window appears, as shown in Figure 8-58.

**Figure 8-58 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: mpls-mvrfce-pe-noc

Description:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="text"/>	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Add	Details...

Rows per page: 10 Go to page: 1 of 1

Add Link Delete Link Save Cancel

**Step 12** Click **Add** in the Link Attribute cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 8-59.

**Figure 8-59 MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>PE Information</b>	
PE	mlpe2
Interface Name:	FastEthernet0/0.
Interface Description:	
Shutdown Interface:	<input type="checkbox"/>
Encapsulation:	DOT1Q
VLAN ID *:	550 (1-4095)
<b>MVRFCE PE Facing Information</b>	
MVRFCE	mlce3
Interface Name:	Ethernet0/1.
Interface Description:	
Encapsulation:	DOT1Q

Note: \* - Required Field

- Step 1 of 7 -

< Back Next > Finish Cancel

**PE Information**

**Step 13 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

**Step 14 VLAN ID:** Enter the *PE VLAN ID*. (**550**)

**MVRFCE PE Facing Information**

**Step 15 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

**Step 16** Click **Next**.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 8-60.

**Figure 8-60 MPLS Link Attribute Editor - Interface**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>MVRFCE CE Facing Information</b>	
MVRFCE	mlce3
Interface Name:	Ethernet0/2: <input type="text"/>
Interface Description:	<input type="text"/>
CE Encapsulation: ⓘ	DOT1Q ▾
VLAN ID *	570 (1-4095)

Note: \* - Required Field

- Step 2 of 7 -

< Back Next > Finish Cancel

**MVRFCE CE Information**

**Step 17 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

**Step 18 VLAN ID:** Enter the *PE VLAN ID*. (**570**)

**MVRFCE PE Facing Information**

**Step 19 Encapsulation:** Choose the PE Encapsulation from the drop-down box. (**DOT1Q**)

Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 8-61.

**Figure 8-61 MPLS Link Attribute Editor - IP Address Scheme**

**MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>PE-MVRFCE Interface Address/Mask</b>	
IP Numbering Scheme:	IP Numbered ▾
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool ▾

Note: \* - Required Field

**Step 20** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears, as shown in Figure 8-62.

**Figure 8-62 MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>MVRFCE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered ▾
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool ▾

Note: \* - Required Field

101717

Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 8-63.

**Figure 8-63 MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>PE-MVRFCE Routing Information</b>	
Routing Protocol	STATIC ▾
Give Only Default Routes to MVRFCE:	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>
Default Information Originate (BGP only):	<input type="checkbox"/>
Advertised Routes for MVRFCE:	Edit
Routes To Reach Other Sites:	Edit

Note: \* - Required Field

101718

**Step 21** Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears, as shown in Figure 8-64.

**Figure 8-64 MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>MVRFCE-CE Routing Information</b>	
Routing Protocol	STATIC ▾
Give Only Default Routes to CE:	<input type="checkbox"/>
Advertised Routes for CE:	Edit
Routes To Reach Other Sites:	Edit

Note: \* - Required Field

101719

Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears, as shown in Figure 8-65.

**Figure 8-65 MPLS Link Attribute Editor - VRF and VPN**

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value				
<b>VRF Information</b>					
Export Map:	<input type="text"/>				
Import Map:	<input type="text"/>				
Maximum Routes:	<input type="text"/> (1-4294967295)				
Maximum Route Threshold *:	<input type="text"/> 80 (1-100)				
VRF Description:	<input type="text"/>				
Allocate new route distinguisher:	<input type="checkbox"/>				
VRF And RD Overwrite	<input type="checkbox"/>				
<b>VPN Selection</b>					
PE VPN Membership *:					
Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	CUST-A	west-xVPN	PROVIDER-X	Default	<input checked="" type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/>					

Note: \* - Required Field

- Step 7 of 7 -

**Step 22** Click **Add** to join VPN.

**Step 23** Click **Finish**.

The MPLS Service Request Editor window reappears, as shown in Figure 8-66.

**Figure 8-66 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: mpls-mvrfce-pe-noce

Description:

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="text"/>	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Edited	Details...

Rows per page:

Go to page:  of 1

**Step 24** Enter the Service Request *description* and click **Save**. (**mpls-mvrfce-pe-noce**)

The MPLS Service Requests window reappears, as shown in Figure 8-67.

**Figure 8-67 Service Request**

**Service Requests**

Show Services with  matching  of type

Showing 1-5 of 5 records

#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	<input type="checkbox"/>	1	DEPLOYED	MPLS	ADD	admin	CUST-A	mpls-pe-ce	10/10/03 4:26 PM	ce2-sw1-sw2-pe2
2.	<input type="checkbox"/>	2	REQUESTED	MPLS	ADD	admin	CUST-A	mpls-pe-ce	10/12/03 12:46 AM	mpls-pe-ce
3.	<input type="checkbox"/>	6	REQUESTED	MPLS	ADD	admin	CUST-A	mpls-pe-noce	10/12/03 9:06 PM	mpls-pe-noce
4.	<input type="checkbox"/>	7	REQUESTED	MPLS	MODIFY	admin	CUST-A	mpls-mvrfce-pe-ce	10/14/03 3:38 PM	mpls-mvrfce-pe-ce
5.	<input type="checkbox"/>	10	REQUESTED	MPLS	ADD	admin	CUST-A	mpls-mvrfce-pe-noce	10/14/03 6:26 PM	mpls-mvrfce-pe-noce

Rows per page:

Auto Refresh: ☒

101722

The MPLS VPN MVRFCE PE-NoCE Service Request is in the Requested state and ready to deploy.





## Provisioning Management VPN

---

This chapter describes how to implement the IP Solutions Center (ISC) Management VPN. This chapter contains the following major sections:

- Overview of the ISC Management Network, page 9-1
- Provisioning a Management CE in ISC, page 9-7

### Overview of the ISC Management Network

This section provides the fundamental concepts and considerations for administering customer edge routers (CEs) in the context of an ISC management subnet. Before ISC can be appropriately deployed to deliver services to customers, the question of whether the CEs are to be managed by the Service Provider or not must be answered

This section contains the following sections:

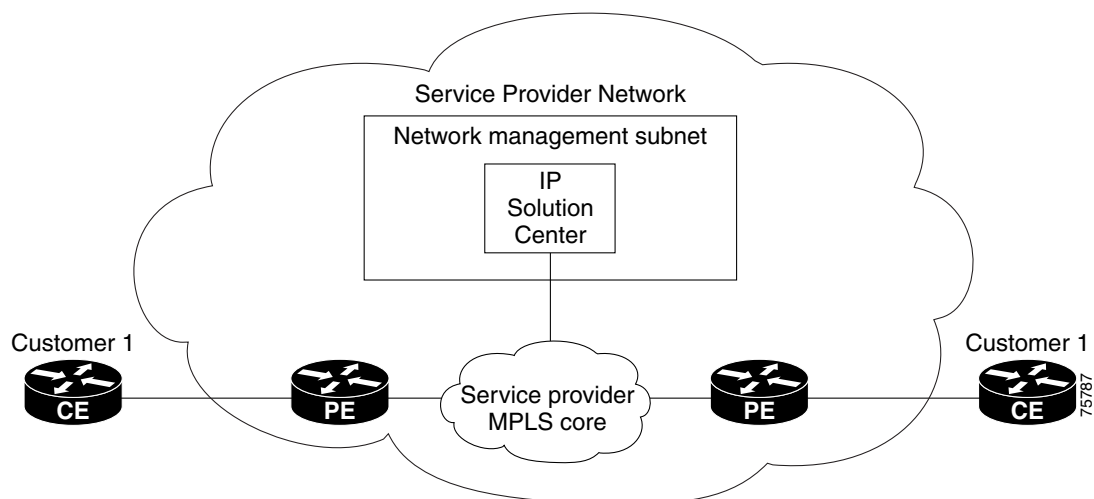
- Unmanaged Customer Edge Routers, page 9-1
- Managed Customer Edge Routers, page 9-2
- Network Management Subnets, page 9-3
- Implementation Techniques, page 9-4
- Out-of-Band Technique, page 9-7

### Unmanaged Customer Edge Routers

One of the options available to the Service Provider is to not manage the customer edge routers (CEs) connected to the Service Provider network. For the Service Provider, the primary advantage of an unmanaged CE is administrative simplicity.

If the CEs are unmanaged, the provider can use IPv4 connectivity for all management traffic. ISC is not employed for provisioning or managing unmanaged CEs.

Figure 9-1 shows a basic topology with unmanaged CEs. The network management subnet has a direct link to the Service Provider MPLS core network.

**Figure 9-1 Service Provider Network and Unmanaged CEs**

Regarding unmanaged CEs, Service Providers should note the following considerations:

- Because unmanaged CEs are outside the Service Provider's administrative domain, the Service Provider does not maintain or configure unmanaged CEs.
- The Service Provider does *not* administer the following elements on the unmanaged CE:
  - IP addresses
  - Host name
  - Domain Name server
  - Fault management (and timestamp coordination by means of the Network Time Protocol)
  - Collecting, archiving, and restoring CE configurations
  - Access data such as passwords and SNMP strings on the unmanaged CE
- Prototype CE configlets are generated, but they are not automatically downloaded to the router.
- There is no configuration management.
  - With no configuration management, no configuration history is maintained and there is no configuration change management.
  - Changes to a service request (on the PE-CE link) are not deployed to the CE.
- There is no configuration auditing because there is no means to retrieve the current CE configuration.
- You can perform routing auditing.
- You can use the Service Assurance Agent (SA Agent) to measure response times between shadow routers, but you *cannot* use SA Agent to measure response times between CEs.

## Managed Customer Edge Routers

The alternative to unmanaged CEs is managed CEs, that is, customer edge routers managed by the Service Provider. Managed CEs can be wholly within the Service Provider's administrative domain or co-managed between the provider and the customer, although CE co-management poses a number of ongoing administrative challenges and is not recommended.

Regarding managed CEs, Service Providers should note the following considerations:

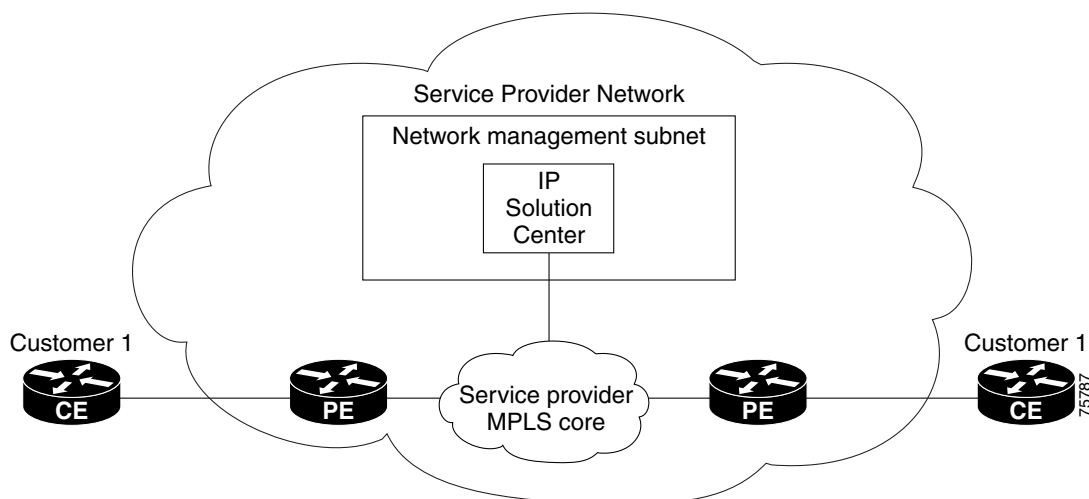
- Managed CEs are within the Service Provider's administrative domain. Thus, some connectivity to the CEs from the Service Provider network is required.
- The Service Provider must administer the following elements on the managed CE:
  - IP addresses
  - Host name
  - Domain Name server
  - Access data such as passwords and SNMP strings
- The Service Provider should administer fault management (and timestamp coordination by means of the Network Time Protocol)
- The Service Provider can administer collecting, archiving, and restoring CE configurations.
- CE configlets are generated and downloaded to the managed CE.
- Changes to service requests are based on the current CE configuration and automatically downloaded.
- The CE configurations are audited.
- Customer routing and Service Provider routing must interact.
- Access from CEs to the management hosts on the network management subnet is required.
- Configuration auditing and routing auditing are both functional.
- You can use the Service Assurance Agent (SA Agent) to measure response times between CEs and between shadow routers.

The following sections discuss the concepts and issues required for administering a managed CE environment.

## Network Management Subnets

The Network Management Subnet is required when the provider's service offering entails the management of CEs. Once a CE is in a VPN, it is no longer accessible by means of conventional IPv4 routing unless one of the techniques described in this chapter is employed.

Figure 9-2 shows the ISC network management subnet and the devices that might be required to connect to it:

**Figure 9-2 The ISC Network Management Subnet**

## Issues Regarding Access to VPNs

The core issues with regard to gaining access to VPNs are as follows:

- How to keep provider space “clean” from unnecessary customer routes
- How to keep customer space “clean” from both the provider’s and other customer’s routes
- How to provide effective security
- How to prevent routing loops

ISC does not handle any of these responsibilities—doing so must be designed and implemented by the Service Provider.

- Reachability changes as a direct consequence of employing ISC.

Before you provision a CE in the ISC, you might be able to reach the CE via IPv4 connectivity, but the moment the product deploys a service request, you cannot reach that CE any more—unless you have *first* implemented the network management subnet.

## Implementation Techniques

The network management subnet must have access to a Management CE (MCE) and PEs.

The network management subnet is appropriate—and necessary—when there is an intent to have managed CEs connected via an in-band connection. *In-band* indicates a single link or permanent virtual circuit (PVC) that carries *both* the customer’s VPN traffic, as well as the provider’s network management traffic.

### Management CE (MCE)

The network management subnet is connected to the Management CE (MCE). The MCE *emulates* the role of a customer edge router (CE), but the MCE is in provider space and serves as a network operations center gateway router. The MCE is part of a management site as defined in the ISC.

You configure the MCE by identifying the CE as part of the management LAN in ISC.

## Management PE (MPE)

The Management PE (MPE) *emulates* the role of a PE in the provider core network. The MPE connects the MCE to the provider core network. An MPE can have a dual role as both a PE and the MPE.

The MPE needs access to the following devices:

Device	Connectivity	Function
1. Customer Edge Routers (CEs)	Access from the network management subnet into the VPNs	Provision or change configuration and collect SA Agent performance data
2. Shadow CEs	Access from the network management subnet into the VPNs	A simulated CE used to measure data travel time between two devices. A shadow CE is connected directly to a PE via Ethernet.
3. Provider Edge Routers (PEs)	Standard IP connectivity	Provision or change configuration

At the current time, ISC recommends two main network management subnet implementation techniques:

- *Management VPN Technique*

The MPE-MCE link uses a Management VPN (see Management VPN, page 9-5) to connect to managed CEs. To connect to the PEs, the MPE-MCE link uses a parallel IPv4 link.

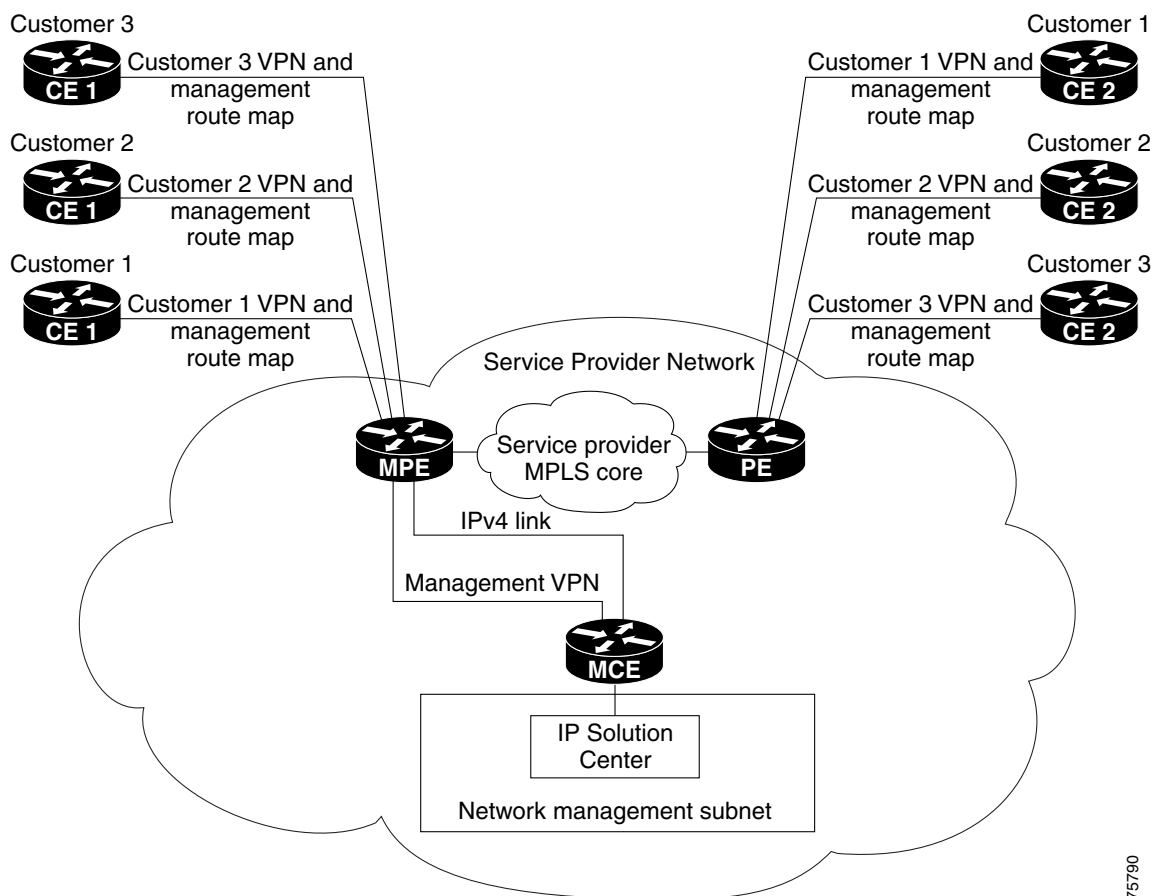
- *Out-of-Band Technique*

In the Out-of-Band technique, the MCE has IPv4 connectivity (that is, not MPLS VPN connectivity) to all the CEs and PEs in the network (see Out-of-Band Technique, page 9-7). In this context, *out-of-band* signifies a separate link between PEs that carries the provider's management traffic.

The network management subnet technique the provider chooses to implement depends on many factors, which are discussed later in this chapter.

## Management VPN

The Management VPN technique is the default method provisioned by ISC. A key concept for this implementation technique is that *all the CEs in the network are a member of the management VPN*. To connect to the PEs, the MPE-MCE link uses a parallel IPv4 link. Figure 9-3 shows a typical topology for the Management VPN technique.

**Figure 9-3** Typical Topology for a Management VPN Network

When employing the Management VPN technique, the MPE-MCE link uses a *management VPN* to connect to managed CEs. To connect to the PEs, the MPE-MCE link employs a parallel IPv4 link.

Each CE in a customer VPN is also added to the management VPN by selecting the **Join the management VPN** option in the service request user interface.

The function of the management route map is to allow only the routes to the specific CE into the management VPN. The Cisco IOS supports only one export route map and one import route map per VRF.

As shown in Figure 9-3, a second parallel non-MPLS VPN link is required between the MPE and MCE to reach the PEs.

**Note**

Implementation of the Management VPN technique requires Cisco IOS 12.07 or higher.

## Advantages

The advantages involved in implementing the Management VPN technique are as follows:

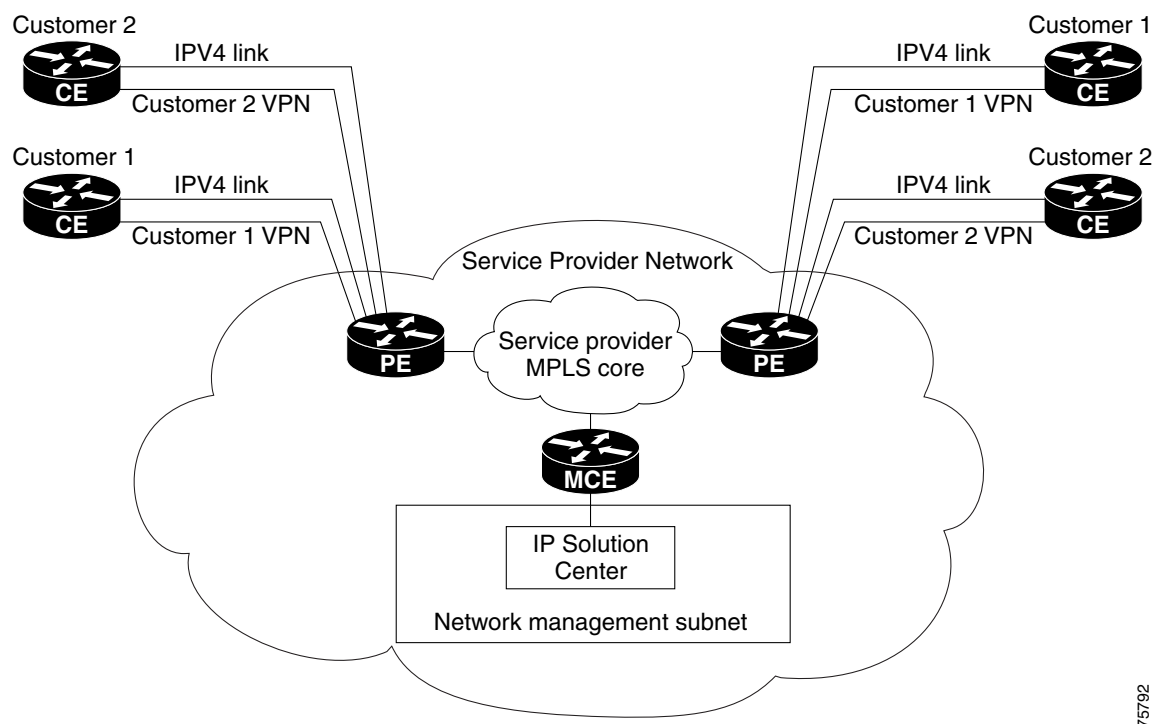
- Provisioning with this method requires only one service request.
- The only routes given to the network management subnet are the routes to the CEs—that is, either the address of the CE link to the PE or the CE loopback address. General VPN routes are *not* given to the network management subnet.

- A CE in the Management VPN method is a spoke to the Management VPN regardless of which role the CE has within its own VPN. Therefore, CEs cannot be accidentally exposed to inappropriate routes. The only management routes the CEs can learn must come from a hub of the Management VPN.

## Out-of-Band Technique

The Out-of-Band technique does not employ a management VPN to manage the CEs. Out-of-band connectivity is provided by IPv4 links. *Out-of-band* signifies a separate link between PEs that carries the provider's management traffic. As shown in Figure 9-4, the MCE provides separation between the provider's routes and the customer's routes.

**Figure 9-4** Out-of-Band Technique



The Out-of-Band technique has the advantage of being relatively simple to set up, and no management VPN is required. However, its disadvantages are that it is expensive since it requires an IPv4 connection to each CE. Also, due to the delicate staging requirements for this technique, the Out-of-Band implementation does have a high degree of complexity.

## Provisioning a Management CE in ISC

The ISC network management subnet is connected to the Management CE (MCE). The MCE *emulates* the role of a customer edge router (CE), but the MCE is in provider space and serves as a network operations center gateway router. The MCE is part of a management site as defined in ISC.

This section contains the following sections:

- Defining a CE as an MCE, page 9-8

- Creating an MCE Service Request, page 9-9

## Defining a CE as an MCE

You configure the MCE by identifying the CE as part of the management LAN in ISC software. To define a CE as an MCE, follow these steps:

- Step 1** Start up and log in to ISC.
- Step 2** From the Welcome to ISC window, choose **Service Inventory**.
- Step 3** From the Service Inventory window, choose **Inventory and Connection Manager**.
- Step 4** From the TOC (table of contents) displayed on the left side of the Inventory and Connection Manager window, choose **CPE Devices**.

The list of CPE devices for all currently defined customers is displayed (see Figure 9-5).

**Figure 9-5** List of All CPEs for All Customers

**CPE Devices**

Show CPEs with  matching

Showing 1-10 of 14 records

#	<input type="checkbox"/>	Device Name	Customer Name	Site Name	Management Type
1.	<input type="checkbox"/>	mlce1.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
2.	<input type="checkbox"/>	mlce2.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
3.	<input type="checkbox"/>	mlce8.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
4.	<input type="checkbox"/>	mlce9.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
5.	<input type="checkbox"/>	mlsw3.cisco.com	AcmeInc	Acme_SF	Multi-VRF - No SA Agent
6.	<input type="checkbox"/>	mlce12.cisco.com	AcmeInc	Acme_TX	Managed - No SA Agent
7.	<input type="checkbox"/>	mlce13.cisco.com	AcmeInc	Acme_TX	Managed - No SA Agent
8.	<input type="checkbox"/>	mlce3.cisco.com	WidgetsInc	Widgets_SF	Multi-VRF - No SA Agent
9.	<input type="checkbox"/>	mlsw3CE.cisco.com	WidgetsInc	Widgets_SF	Managed - No SA Agent
10.	<input type="checkbox"/>	mlce4.cisco.com	WidgetsInc	Widgets_NY	Managed - No SA Agent

Rows per page:  << Page 1, 2 >>

- Step 5** Choose the CE that will function as the MCE in the management VPN, then click **Edit**.

The Edit CPE Device dialog box appears, displaying the pertinent information for the selected CPE (see Figure 9-6).

**Figure 9-6** Editing the Selected CPE Device

**Edit CPE Device**

Device Name: mlce8.cisco.com

Site Name: Acme\_SF

Customer Name: AcmeInc

Management Type: Managed - Management LAN

Wildcard Preshare Key:

IP Address Ranges:

Showing 1-5 of 11 records

#	Name	IP Address	IP Address Type	Encapsulation	Description	IPsec	Firewall	NAT	QoS Candidate
1.	ATM3/0		STATIC	UNKNOWN		None	None	None	None
2.	ATM3/1		STATIC	UNKNOWN		None	None	None	None
3.	ATM3/2		STATIC	UNKNOWN		None	None	None	None
4.	FastEthernet0/0	172.29.146.31/26	STATIC	UNKNOWN	CONNECTION TO MLGW1 - DO NOT TOUCH	None	None	None	None
5.	FastEthernet0/1		STATIC	UNKNOWN	L7: Link To mls3	None	None	None	None

Rows per page: 5

<< Page 1, 2, 3 >>

**Step 6** *Management Type:* From the drop-down list, set the management type to **Managed—Management LAN**.

**Step 7** Click **Save**.

You return to the list of CPE devices, where the new management type for the selected CE (in our example, 3. *mlce8.cisco.com*) is now displayed (see Figure 9-7).

**Figure 9-7** Selected CE Defined as a Management CE

**CPE Devices**

Show CPEs with  matching

Showing 1-5 of 14 records

#	<input type="checkbox"/>	Device Name	Customer Name	Site Name	Management Type
1.	<input type="checkbox"/>	mlce1.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
2.	<input type="checkbox"/>	mlce2.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
3.	<input type="checkbox"/>	mlce8.cisco.com	AcmeInc	Acme_SF	Managed - Management LAN
4.	<input type="checkbox"/>	mlce9.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
5.	<input type="checkbox"/>	mlsw3.cisco.com	AcmeInc	Acme_SF	Multi-VRF - No SA Agent

## Creating an MCE Service Request

To create an MCE service request, follow these steps:

- Step 1** Start up and Log in to ISC.
- From the Welcome to ISC window, choose **Service Inventory**.

- b. From the Service Inventory window, choose **Inventory and Connection Manager**.
- c. From the Inventory and Connection Manager window, choose **Service Requests**.

The Service Requests dialog box appears (see Figure 9-8).

**Figure 9-8 Initial Service Requests Dialog Box**

- Step 2** To start the process to create a new service, click **Create**.

A drop-down list is displayed, showing the types of service requests you can create.

- Step 3** Choose **MPLS VPN**.

The Select MPLS Policy dialog box appears (see Figure 9-9).

This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

**Figure 9-9 Selecting the MPLS Policy for This Service**

- Step 4** Choose the policy of choice, then click **OK**.

The MPLS Service Request Editor appears (see Figure 9-10).

**Figure 9-10 MPLS Service Request Editor**

**MPLS Service Request Editor**

Job ID:                      SR ID:                      SR State:

Policy:      acme\_mgmt\_pe\_ce

Description:

Showing 0 of 0 records

#	<input checked="" type="checkbox"/>	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
Rows per page: 10								

Add Link   Delete Link   Save   Cancel

**Step 5** Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields, as shown in Figure 9-11. Notice that the *Select CE* field is enabled. Specifying the CE for the link is the first task required to define the link for this service.

**Figure 9-11 Initial Fields Displayed to Define PE-CE Link**

#	<input type="checkbox"/>	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CE	<input type="text"/>	Select PE	<input type="text"/>	Add	N/A

Rows per page: 10

Add Link   Delete Link   Save   Cancel

**Step 6** *CE*: Click **Select CE**.

The Select CPE Device dialog box is displayed (see Figure 9-12).

**Figure 9-12** *Selecting the MCE for the MPLS Link*

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	<input type="radio"/>	mlce1.cisco.com	AcmeInc	Acme_NY	MANAGED
2.	<input type="radio"/>	mlce2.cisco.com	AcmeInc	Acme_NY	MANAGED
3.	<input checked="" type="radio"/>	mlce8.cisco.com	AcmeInc	Acme_SF	MANAGED_MGMT_LAN
4.	<input type="radio"/>	mlce9.cisco.com	AcmeInc	Acme_SF	MANAGED

- From the *Show CPEs with* drop-down list, you can display CEs by *Customer Name*, by *Site*, or by *Device Name*.
- You can use the **Find** button to either search for a specific CE, or to refresh the display.
- You can set the *Rows per page* to **5**, **10**, **20**, **30**, **40**, or **All**.
- This dialog box displays the first page of the list of currently defined CE devices. The number of pages of information is displayed in the lower right corner of the dialog box.

To go to the another page of CE devices, click the number of the page you want to go to.

**Step 7** In the **Select** column, choose the name of the MCE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected CE is now displayed in the CE column.

**Step 8** *CE Interface*: Choose the CE interface from the drop-down list (see Figure 9-13).

**Figure 9-13** *CE and CE Interface Fields Defined*

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce8	FastEthernet1/0	Select PE		Add	N/A

Note that in the PE column, the **Select PE** option is now enabled.

**Step 9** *PE*: Click **Select PE**.

The Select PE Device dialog box is displayed (see Figure 9-14).

**Figure 9-14** *Selecting the PE for the MPLS Link*

PE for MPLS VPN Link

Show PEs with **Provider Name** matching

Showing 1-4 of 4 records

#	Select	Device Name	Provider Name	Region Name	Role Type
1.	<input checked="" type="radio"/>	mlpe1.cisco.com	FirstProvider	US	PE_POP
2.	<input type="radio"/>	mlpe2.cisco.com	FirstProvider	US	PE_POP
3.	<input type="radio"/>	mlpe3.cisco.com	FirstProvider	US	PE_POP
4.	<input type="radio"/>	mlpe4.cisco.com	FirstProvider	US	PE_POP

Rows per page:

**Step 10** In the Select column, choose the name of the PE for the MPLS link, then click **Select**.

You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.

**Step 11** *PE Interface*: Choose the PE interface from the drop-down list (see Figure 9-15).

**Figure 9-15** *PE and PE Interface Fields Defined*

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input checked="" type="checkbox"/>	0	mlce8	<input type="text" value="FastEthernet1/0"/>	mlpe1	<input type="text" value="FastEthernet1/0"/>	Add	N/A

Rows per page:

Note that the Link Attribute **Add** option is now enabled.

**Step 12** In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor is displayed, showing the fields for the interface parameters (see Figure 9-16).

**Figure 9-16** Specifying the MPLS Link Interface Attributes

MPLS Link Attribute Editor - Interface	
Attribute	Value
<b>PE Information</b>	
PE	mlpe1
Interface Name *	FastEthernet1/0
Interface Description:	
Shutdown Interface:	<input type="checkbox"/>
Encapsulation:	DOT1Q
Auto-Pick Vlan ID:	<input checked="" type="checkbox"/>
<b>CE Information</b>	
CE	mlce8
Interface Name *	FastEthernet1/0
Interface Description:	
Encapsulation:	DOT1Q

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on each of the PE and CE interface fields, see Specifying PE and CE Interface Parameters, page 5-8.

**Note**

The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both.

- Step 13** Edit any interface values that need to be modified for this particular link, then click **Next**.  
The MPLS Link Attribute Editor for the IP Address Scheme appears (see Figure 9-17).

**Figure 9-17** Specifying the MPLS Link IP Address Attributes

MPLS Link Attribute Editor - IP Address Scheme	
Attribute	Value
<b>PE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered
Extra CE Loopback Required:	<input type="checkbox"/>
Automatically Assign IP Addresses:	<input checked="" type="checkbox"/>
IP Address Pool:	Region Pool

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the IP address scheme fields, see Specifying IP Address Scheme, page 5-12.

- Step 14** Edit any IP address scheme values that need to be modified for this particular link, then click **Next**.  
The MPLS Link Attribute Editor for Routing Information appears (see Figure 9-18).

**Figure 9-18 Specifying the MPLS Link Routing Protocol Attributes**

MPLS Link Attribute Editor - Routing Information	
Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	BGP
Redistribute Static (BGP only):	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input checked="" type="checkbox"/>
CE BGP AS ID *	200 (1-65535)
Neighbor Allow-AS in:	3 (1-10)
Neighbor AS Override:	<input type="checkbox"/>
Redistributed Protocols on CE:	Edit

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the routing information for the PE and CE, see *Specifying Routing Protocol for a Service*, page 5-15.

Because the service policy used for this service specified the routing protocol as editable, you can change the routing protocol for this service request as needed.

- Step 15** Edit any routing protocol values that need to be modified for this particular link, then click **Next**.  
The MPLS Link Attribute Editor for the VRF and VPN attributes appears (see Figure 9-19).

**Figure 9-19 Specifying the MPLS Link VRF and VPN Attributes**

MPLS Link Attribute Editor - VRF and VPN	
Attribute	Value
<b>VRF Information</b>	
Export Map:	
Import Map:	
Maximum Routes:	(1-4294967295)
Maximum Route Threshold *	80 (1-100)
VRF Description:	

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service. For details on the VRF and VPN information, see *Defining the Service Policy VRF and VPN Information*, page 5-39.

- Step 16** Edit any VRF values that need to be modified for this particular link, then click **Finish**.

You return to the MPLS Service Request Editor.

- Step 17** To save your work on this first link in the service request, click **Save**.

You return to the Service Requests dialog box, where the information for the link you just defined is now displayed (see Figure 9-20).

**Figure 9-20 Service Request for an MPLS Link Completed**

**Service Requests**

Show Services with Job ID  matching \*  of type All  Find

Showing 1-1 of 1 records

#	<input type="checkbox"/>	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	<input type="checkbox"/>	12	REQUESTED	MPLS	ADD	admin	AcmeInc	acme_mgmt_pe_ce	6/19/03 3:33 PM	

Rows per page:

Auto Refresh: ☒

Create ▼ Details Edit Deploy ▼ Decommission Purge ▼

95376

You can add additional links to this service request by choosing **Add Link** and specifying the attributes of the next link in the service. As you can see, the service request is in the *Requested* state. When all the links for this service have been defined, you must deploy the service.

## Adding PE-CE Links to the Management VPN

When you have created the Management VPN, then you can proceed to add service for the PE-CE links you want to participate in the Management VPN.

To add PE-CE links, follow these steps:

- Step 1** Navigate to the MPLS Link Attribute Editor - VRF and VPN window for the selected CE.
- Step 2** Check the **Join the management VPN** option, as shown in Figure 9-21.

**Figure 9-21 Joining a CE to the Management VPN**

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value				
<b>VRF Information</b>					
Export Map:	<input type="text"/>				
Import Map:	<input type="text"/>				
Maximum Routes:	<input type="text"/> (1-4294967295)				
Maximum Route Threshold %:	<input type="text"/> 80 (1-100)				
VRF Description:	<input type="text"/>				
Allocate new route distinguisher:	<input type="checkbox"/>				
VRF And RD Overwrite	<input type="checkbox"/>				
Join the management VPN:	<input checked="" type="checkbox"/>				
<b>VPN Selection</b>					
PE VPN Membership %:	<input type="text"/>				
Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	AcmeInc	AcmeIncVPN	FirstProvider	Default	<input checked="" type="checkbox"/>

Add Delete

95377

When you join the CE with the Management VPN in this step, ISC generates the appropriate route-map statements in the PE configlet.

The function of the management route map is to allow only the routes to the specific CE into the management VPN. Cisco IOS supports only one export route map and one import route map per VRF (and therefore, per VPN).

**Step 3** Complete the service request user interface.

---





## Provisioning Cable Services

---

This chapter describes how to provision MPLS VPN cable in IP Solutions Center (ISC). This chapter contains the following major sections:

- Overview of MPLS VPN Cable, page 10-1
- Provisioning Cable Services in ISC, page 10-6
- Creating the Service Requests, page 10-6

### Overview of MPLS VPN Cable

Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared Hybrid Fiber Coaxial (HFC) network and Internet Protocol (IP) infrastructure. The cable MPLS VPN network consists of the following two major elements:

- The Multiple Service Operator (MSO) or cable company that owns the physical infrastructure and builds VPNs for the Internet Service Providers (ISPs) to move traffic over the cable and IP backbone.
- ISPs that use the HFC network and IP infrastructure to supply Internet service to cable customers.

### Benefits of Cable MPLS VPNs

Provisioning cable services with MPLS VPNs provides the following benefits:

- MPLS VPNs give cable MSOs and ISPs a manageable way of supporting multiple access to a cable plant.

Service providers can create scalable and efficient VPNs across the core of their networks. MPLS VPNs provide systems support scalability in cable transport infrastructure and management.

- Each ISP can support Internet access services from a subscriber's PC through an MSO's physical cable plant to their networks.
- MPLS VPNs allow MSOs to deliver value-added services through an ISP, and thus, deliver connectivity to a wider set of potential customers.

MSOs can partner with ISPs to deliver multiple services from multiple ISPs and add value within the MSO's own network using VPN technology.

- Subscribers can choose combinations of services from various service providers.

- The Cisco IOS MPLS VPN cable feature sets build on Cable Modem Termination Server (CMTS) and DOCSIS 1.0 extensions to ensure services are reliably and optimally delivered over the cable plant.  
MPLS VPN provides systems support domain selection, authentication per subscriber, selection of QoS, policy-based routing, and ability to reach behind the cable modem to subscriber end-devices for QoS and billing, while preventing session-spoofing.
- MPLS VPN technology ensures both secure access across the shared cable infrastructure and service integrity.

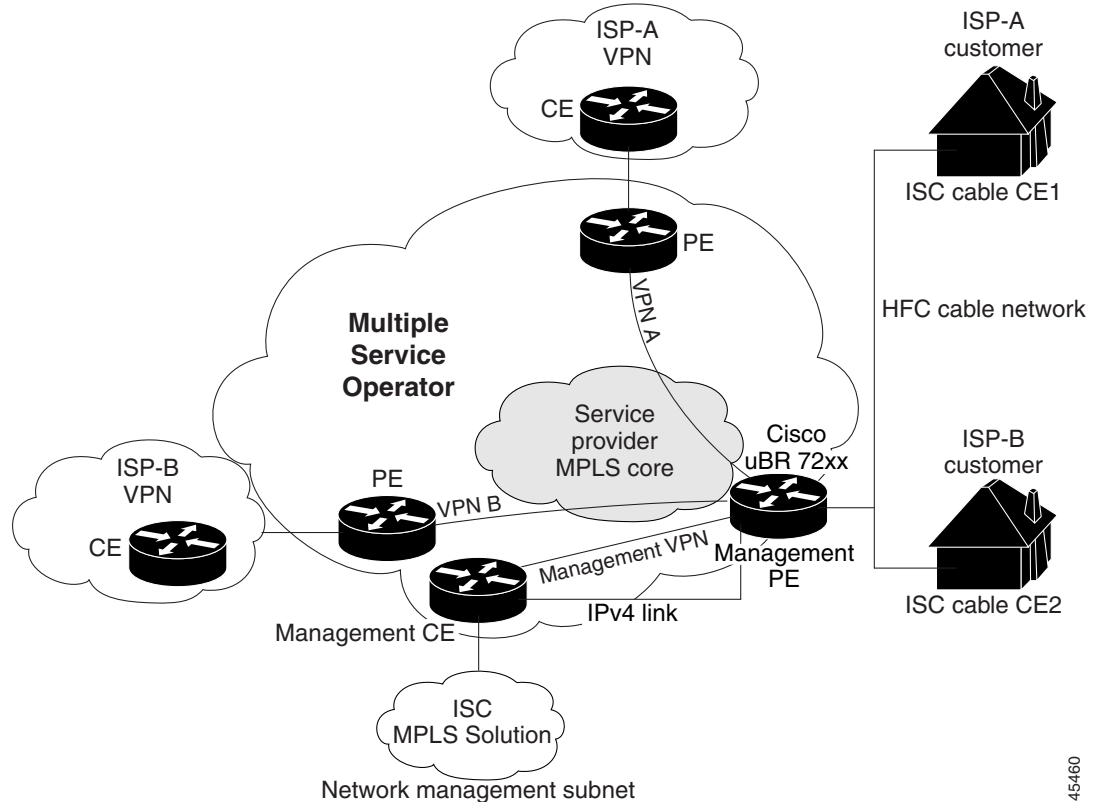
## The Cable MPLS VPN Network

As shown in Figure 10-1, each ISP moves traffic to and from a subscriber's PC, through the MSO's physical network infrastructure, to the ISP's network. MPLS VPNs, created in Layer 3, provide privacy and security by constraining the distribution of VPN routes only to the routers that belong to its network. Thus, each ISP's VPN is insulated from other ISPs that use the same MSO infrastructure.

In the MPLS-based cable scheme, a VPN is a private network built over a shared cable plant and MPLS-core backbone. The public network is the shared cable plant or backbone connection points. A cable plant can support Internet access services and carry traffic for an MSO and its subscribers, as well as for multiple Internet Service Providers (ISPs) and their subscribers.

An MPLS VPN assigns a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine the contents of the forwarding table.

Each PE router maintains one or more VRF tables. If a packet arrives directly through an interface associated with a particular VRF, the PE looks up a packet's IP destination address in the appropriate VRF table. MPLS VPNs use a combination of BGP and IP address resolution to ensure security.

**Figure 10-1 Example of an MPLS VPN Cable Network**

45460

The routers in the cable network are as follows:

- **Provider (P) router**—Routers in the MPLS core of the service provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS labels in each route assigned by the PE router) to routed packets. VPN labels direct data packets to the correct egress router.
- **Provider Edge (PE) router**—A router that attaches the VPN label to incoming packets based on the interface or subinterface on which they are received. A PE router attaches directly to a CE router. In the MPLS-VPN approach, each Cisco uBR72xx series router acts as a PE router.
- **Customer (C) router**—A router in the ISP or enterprise network.
- **Customer Edge (CE) router**—Edge router on the ISP's network that connects to the PE router on the MSO's network. A CE router must interface with a PE router.
- **Management CE (MCE) router**—The MCE *emulates* the role of a customer edge router (CE), but the MCE is in provider space and serves as a network operations center gateway router. The network management subnet is connected to the Management CE (MCE). The MCE is part of a management site as defined in the ISC.
- **Management PE (MPE) router**—The MPE *emulates* the role of a PE in the provider core network. The MPE connects the MCE to the provider core network. An MPE can have a dual role as both a PE and the MPE.

The shared cable plant supports Internet connectivity from ISP A to its subscribers and from ISP B to its subscribers.

## Management VPN in the Cable Network

The MPLS network has a unique VPN that exclusively manages the MSOs devices called the *management VPN*. It contains servers and devices that other VPNs can access. The management VPN connects the Management CE (MCE) router and the management subnet to the MSO PE router (a uBr72xx router or equivalent). ISC and the management servers, such as Dynamic Host Configuration Protocol (DHCP), Cisco Network Registrar (CNR) Time of Day (ToD) are part of the management subnet and are within the management VPN for ISP connectivity. For an explanation of the management VPN, see Chapter 9, “Provisioning Management VPN.”

As shown in Figure 10-1, the management VPN is comprised of the network management subnet (where the ISC workstation resides), which is directly connected to the Management CE (MCE). The management VPN is a special VPN between the MCE and the cable VPN gateway. The cable VPN gateway is usually a Cisco uBR 72xx router that functions as both a regular PE and a Management PE. Notice that there is also a parallel IPv4 link between the MCE and the MPE.

## Cable VPN Configuration Overview

Cable VPN configuration involves the following:

- An MSO domain that requires a direct peering link to each enterprise network (ISP), provisioning servers for residential and commercial subscribers, and dynamic DNS for commercial users. The MSO manages cable interface IP addressing, Data Over Cable Service Interface Specifications (DOCSIS) provisioning, cable modem hostnames, routing modifications, privilege levels, and usernames and passwords.
- An ISP or enterprise domain that includes the DHCP server for subscriber or telecommuter host devices, enterprise gateway within the MSO address space, and static routes back to the telecommuter subnets.

**Note**

Cisco recommends that the MSO assign all addresses to the end user devices and gateway interfaces. The MSO can also use split management to let the ISP configure tunnels and security.

To configure MPLS VPNs for cable services, the MSO must configure the following:

- Cable Modem Termination System (CMTS)

The CMTS is usually a Cisco uBR72xx series router. The MSO must configure Cisco uBR72xx series routers that serve the ISP.

- PE routers

The MSO must configure PE routers that connect to the ISP as PEs in the VPN.

**Tip**

When configuring MPLS VPNs for cable services, you must configure the cable maintenance subinterface on the PE. The cable maintenance interface is the means by which the cable device retrieves its own IP address. For this reason, the maintenance subinterface must be configured before cable services provisioning can take place.

- CE routers
- P routers
- One VPN per ISP

- DOCSIS servers for all cable modem customers

The MSO must attach DOCSIS servers to the management VPN and make them visible to the network.

The MSO must determine the *primary IP address range*. The primary IP address range is the MSO's address range for all cable modems that belong to the ISP subscribers.

The ISP must determine the *secondary IP address range*. The secondary IP address is the ISP's address range for its subscriber PCs.

To reduce security breaches and differentiate DHCP requests from cable modems in VPNs or under specific ISP management, MSOs can use the **cable helper-address** command in Cisco IOS software. The MSO can specify the host IP address to be accessible only in the ISP's VPN. This lets the ISP use its DHCP server to allocate IP addresses. Cable modem IP address must be accessible from the management VPN.

In ISC, you specify the maintenance helper address and the host helper address and the secondary addresses for the cable subinterface.

## Cable VPN Interfaces and Subinterfaces

In the cable subscriber environment, several thousand subscribers share a single physical interface. Configurations with multiple logical subinterfaces are a vital part of the MPLS VPN network over cable. You can configure multiple subinterfaces and associate a specific VRF with each subinterface. You can split a single physical interface (the cable plant) into multiple subinterfaces, where each subinterface is associated with a specific VRF. Each ISP requires access on a physical interface and is given its own subinterface. The MSO administrator can define subinterfaces on a cable physical interface and assign Layer 3 configurations to each subinterface.

The MPLS VPN approach of creating VPNs for individual ISPs or customers requires subinterfaces to be configured on the cable interface. One subinterface is required for each ISP. The subinterfaces are tied to the VPN Routing/Forwarding (VRF) tables for their respective ISPs.

You must create the *maintenance subinterface* on the cable interface and tie it to the management VPN. The maintenance interface is for the ISP's use, and it is used for VPN connectivity, as well as the management VPN using an extranet between the ISP and the management VPN.

ISC automatically selects the subinterface number based on the VRF. If a subinterface that is associated with the current VRF does not yet exist, ISC creates a subinterface and assigns it to the correct VRF. The subinterface number is incremented to 1 greater than the largest subinterface currently assigned for the selected cable interface.

The network management subnet (which includes the CNR, ToD, and ISC) can reply to the cable modem because the management VPN allows connectivity for one filtered route from the ISP's VPN to the Management CE (MCE). Similarly, in order to forward the management requests (such as DHCP renewal to CNR), the ISP VPN must import a route to the MCE in the management VPN.

Cisco uBR7200 series software supports the definition of logical network layer interfaces over a cable physical interface. The system supports subinterface creation on a physical cable interface.

Subinterfaces allow traffic to be differentiated on a single physical interface and associated with multiple VPNs. Each ISP requires access on a physical interface and is given its own subinterface. Using each subinterface associated with a specific VPN (and therefore, ISP) subscribers connect to a logical subinterface, which reflects the ISP that provides their subscribed services. Once properly configured, subscriber traffic enters the appropriate subinterface and VPN.

# Provisioning Cable Services in ISC

The tasks you must complete to provision cable services in ISC are as follows:

- Add the PE that has cable interfaces to the appropriate Region.
- Generate a service request to provision the cable maintenance interface on the PE.
- Generate a second service request to provision the MPLS-based cable service. You must generate this cable service request for each VPN.

When using the ISC to provision cable services, there are no CEs in the same sense there are when provisioning a standard MPLS VPN. Thus, you must use a PE-Only (NOCE) policy or create a cable policy with no CE.

## Creating the Service Requests

This section contains the following subsections:

- Creating a Cable Subinterface Service Request, page 10-6
- Creating a Cable Link Service Request, page 10-11

### Creating a Cable Subinterface Service Request

The cable maintenance subinterface on the PE is the means by which the cable device retrieves its own IP address. For this reason, the maintenance subinterface must be configured before provisioning cable services.

To create a cable subinterface service request, follow these steps:

- 
- Step 1** Start up and Log in to ISC.
- a. From the Welcome to ISC window, choose **Service Inventory**.
  - b. From the Service Inventory window, choose **Inventory and Connection Manager**.
  - c. From the Inventory and Connection Manager window, choose **Service Requests**.

The Service Requests dialog box appears.

- Step 2** Click **Create**.

A drop-down list is displayed, showing the types of service requests you can create.

- Step 3** Choose **MPLS VPN**.

The Select MPLS Policy dialog box appears (see Figure 10-2).

This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

**Figure 10-2** Selecting the Cable Policy for the Subinterface

Select MPLS Policy

Show MPLS policies with  Matching

Showing 1 - 3 of 3 records

#	Policy Name	Policy Owner
1. <input checked="" type="radio"/>	cable	Provider - Provider1
2. <input type="radio"/>	mpls-pe-noce	Customer - Customer1
3. <input type="radio"/>	mpls1	Customer - Customer1

Rows per page:

- Step 4** Check the check box for the PE-Only policy (*Cable* in the example above) policy, and then click **OK**. The MPLS Service Request Editor appears (see Figure 10-3).

**Figure 10-3** MPLS Service Request Editor

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: cable

Customer: Select Customer

Description:

Showing 0 of 0 records

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
---	--------------------------	---------	-----	---------------	----	--------------	----------------	--------------

Rows per page:

- Step 5** Click **Add Link**.
- The MPLS Service Request Editor now displays a set of fields. Notice that the *Select PE* field is enabled. Specifying the PE for the link is the first task required to define the link for this service.

- Step 6** *PE*: Click **Select PE**.

The Select PE Device dialog box is displayed (see Figure 10-4).

**Figure 10-4** *Selecting the PE for the MPLS Link*

Showing 1 - 5 of 5 records

#	Device Name	Provider Name	Region Name	Role Type
1.	mlpe2	Provider1	West	PE_POP
2.	mlpe4	Provider1	East	PE_POP
3.	enswosr1	Provider1	West	PE_POP
4.	enswosr2	Provider1	East	PE_POP
5.	enpe1	Provider1	West	PE_POP

Rows per page: 10 Go to page: 1 of 1

Select Cancel

- Step 7** In the Select column, choose the name of the PE for the MPLS link, then click **Select**.  
You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.
- Step 8** *PE Interface:* Choose the PE interface from the drop-down list (see Figure 10-5).

**Figure 10-5** *PE and PE Interface Fields Defined*

Showing 1 - 1 of 1 record

#	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CLE		enpe1	Cable0/1	Add	N/A

Rows per page: 10 Go to page: 1 of 1

Add Link Delete Link Save Cancel

Only the major interface names are available for you to select. ISC assigns the appropriate subinterface number for each VPN.

The Link Attribute **Add** option is now enabled.

- Step 9** In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor is displayed, showing the fields for the interface parameters (see Figure 10-6).

**Figure 10-6** Specifying the MPLS Link Interface Attributes

Attribute	Value
<b>PE Information</b>	
PE	enpe1
Interface Name:	Cable0/1. <input type="text"/>
Interface Description:	<input type="text" value="cable maintenance"/>
Shutdown Interface:	<input checked="" type="checkbox"/>
Cable Maintenance Interface:	<input checked="" type="checkbox"/>
Cable Helper Addresses:	<input type="button" value="Edit"/>

**Step 10** Enter a subinterface name in the Interface Description field.

**Step 11** Check the check box for the Cable Maintenance Interface, then click **Edit** beside Cable Helper Addresses.

The Cable Helper Addresses window appears.

**Step 12** Click **Add**. The Cable Helper Addresses window appears as shown in Figure 10-7.

**Figure 10-7** Cable Helper Addresses

Cable Helper Addresses		
Select	IP Address (a.b.c.d)	IP Type
<input type="checkbox"/>	<input type="text" value="209.165.100.1"/>	<input type="text" value="Both"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>		

**Step 13** Enter an **IP address** in the IP Address field and choose **Both** for IP Type.

Cable Modems and their attached CPE devices (hosts) will broadcast DHCP packets to the destination IP address, and this destination IP address is the configured cable helper address. So, from configured cable helper address, cable modems and their attached CPE (hosts) will receive their (CM and CPE) IP address.

IP Type can have the following values:

- **Host**—When selected, only UDP broadcasts from hosts (CPE devices) are forwarded to that particular destination IP address. (For example, only hosts will receive IP addresses from the mentioned helper address.)
- **Modem**—When selected, only UDP broadcasts from cable modems are forwarded to that particular destination IP address. (For example, only cable modems will receive IP addresses from the mentioned helper address.)
- **Both**—When selected, UDP broadcasts from hosts (CPE devices) and cable modems are forwarded to that particular destination IP address. (For example, both cable modems and hosts will receive IP addresses from the mentioned helper address.)

**Step 14** Click **OK**.

The MPLS Link Attribute Editor reappears.

**Step 15** Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme appears (see Figure 10-8).

**Figure 10-8** Specifying the MPLS Link IP Address Attributes

Attribute	Value
<b>PE-CE Interface Addresses/Mask</b>	
IP Numbering Scheme:	IP Numbered
PE Interface Address/Mask:	10.1.1.1/24 (a.b.c.d/e)

**Step 16** Edit any IP address scheme values that must be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for Routing Information appears (see Figure 10-9).

**Figure 10-9** Specifying the MPLS Link Routing Protocol Attributes

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	NONE
Redistribute Static (BGP only):	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>

The following routing protocol options are supported:

- STATIC
- RIP
- OSPF
- EIGRP
- None

Because the service policy used for this service specified the routing protocol as editable, you can change the routing protocol for this service request as needed.

**Step 17** Edit any routing protocol values that must be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for the VRF and VPN attributes appears (see Figure 10-10)

**Figure 10-10** Specifying the MPLS Link VRF and VPN Attributes

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	<input type="text"/>
Import Map:	<input type="text"/>
Maximum Routes:	<input type="text"/> (1-4294967295)
Maximum Route Threshold *:	<input type="text"/> 80 (1-100)
VRF Description:	<input type="text"/>
Allocate new route distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>
Join the management VPN:	<input checked="" type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	
Select	Customer
<input type="checkbox"/>	Provider_A_Mgmt
	provider_maintenance
	Provider_A
	Default
	Is Hub
	<input type="checkbox"/>

Add Delete

95422

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service.

- Step 18** Check the check box for Join the Management VPN.
- Step 19** Edit any VRF and VPN values that must be modified for this particular link, then click **Finish**.  
You return to the MPLS Service Request Editor.



**Note** You can define multiple links in this service request.

- Step 20** To save your work on this first link in the service request, click **Save**.  
You return to the Service Requests dialog box, where the information for the link you just defined is now displayed.

## Creating a Cable Link Service Request

To create a Cable Link service request, follow these steps:

- Step 1** Start up and log in to ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.  
The Service Requests dialog box appears.
- Step 3** To start the process to create a new service, click **Create**.  
A drop-down list is displayed, showing the types of service requests you can create.
- Step 4** Choose **MPLS VPN**.  
The Select MPLS Policy dialog box appears (see Figure 10-11).

This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

**Figure 10-11** *Selecting the Cable Link Policy for This Service*

**Select MPLS Policy**

Show MPLS policies with  Matching

Showing 1 - 4 of 4 records

#	Policy Name	Policy Owner
1. <input type="radio"/>	cable	Provider - Provider1
2. <input checked="" type="radio"/>	cable1	Global
3. <input type="radio"/>	mpls-pe-noc	Customer - Customer1
4. <input type="radio"/>	mpls1	Customer - Customer1

Rows per page:

Go to page:  of 1

**Step 5** Choose the policy of choice, then click **OK**.

**Step 6** The MPLS Service Request Editor appears. Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields, as shown in Figure 10-12. Note that in the PE column, the **Select PE** option is now enabled.

**Figure 10-12** *MPLS Service Request Editor*

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: cable1

Customer: Select Customer

Description:

Showing 1 - 1 of 1 record

#	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1. <input type="checkbox"/>	0	Select CLE	<input type="text"/>	Select PE	<input type="text"/>	Add	N/A

Rows per page:

Go to page:  of 1

**Step 7** *PE*: Click **Select PE**.

The Select PE Device dialog box is displayed (see Figure 10-13).

**Figure 10-13** Selecting the PE for the MPLS Link

Showing 1 - 5 of 5 records

#	Device Name	Provider Name	Region Name	Role Type
1.	mlpe2	Provider1	West	PE_POP
2.	enswosr1	Provider1	West	PE_POP
3.	enpe1	Provider1	West	PE_POP
4.	mlpe4	Provider1	East	PE_POP
5.	enswosr2	Provider1	East	PE_POP

Rows per page: 10 Go to page: 1 of 1

Select Cancel

- Step 8** In the Select column, choose the name of the PE for the MPLS link, then click **Select**.  
You return to the Service Request Editor window, where the name of the selected PE is now displayed in the PE column.
- Step 9** *PE Interface*: Choose the PE interface from the drop-down list (see Figure 10-14).

**Figure 10-14** PE and PE Interface Fields Defined

Showing 1 - 1 of 1 record

#	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CLE		enpe1	Cable0/1	Add	N/A

Rows per page: 10 Go to page: 1 of 1

Add Link Delete Link Save Cancel

Note that the Link Attribute **Add** option is now enabled.

- Step 10** In the Link Attribute column, click **Add**.  
The MPLS Link Attribute Editor is displayed, showing the fields for the interface parameters (see Figure 10-15).

**Figure 10-15** Specifying the MPLS Link Interface Attributes

Attribute	Value
<b>PE Information</b>	
PE	enpe1
Interface Name *	Cable0/1
Interface Description:	for ISP_1
Shutdown Interface:	<input type="checkbox"/>
Cable Maintenance Interface:	<input type="checkbox"/>
Cable Helper Addresses:	Edit
Secondary Addresses:	Edit

Note: \* - Required Field

**Note**

Do not check the box for Cable Maintenance Interface.

**Step 11** Edit any interface values that must be modified for this particular link, then click **Edit** beside Cable Helper Addresses. The Cable Helper Addresses window appears.

**Step 12** Click **Add**. The Cable Helper Addresses window appears as shown in Figure 10-16.

**Figure 10-16** Cable Helper Addresses

**Step 13** Enter an **IP address** in the IP Address field and choose **Both**, **Modem**, or **Host** for IP Type.

Cable Modems and their attached CPE devices (hosts) will broadcast DHCP packets to the destination IP address, and this destination IP address is the configured cable helper address. So, from configured cable helper address, cable modems and their attached CPE (hosts) will receive their (CM and CPE) IP address.

IP Type can have the following values:

- **Host**—When selected, only UDP broadcasts from hosts (CPE devices) are forwarded to that particular destination IP address. (For example, only hosts will receive IP addresses from the mentioned helper address.)
- **Modem**—When selected, only UDP broadcasts from cable modems are forwarded to that particular destination IP address. (For example, only cable modems will receive IP addresses from the mentioned helper address.)

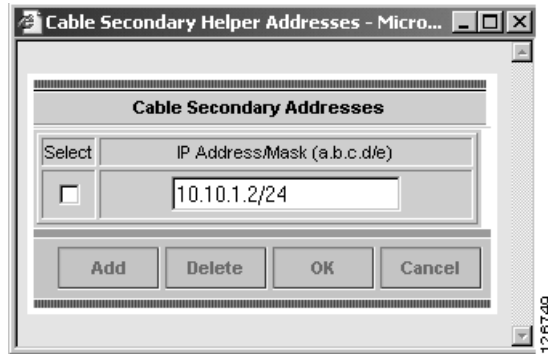
- **Both**—When selected, UDP broadcasts from hosts (CPE devices) and cable modems are forwarded to that particular destination IP address. (For example, both cable modems and hosts will receive IP addresses from the mentioned helper address.)

**Step 14** Click **OK**. The MPLS Link Attribute Editor reappears.

**Step 15** Click **Edit** beside Secondary Addresses. The Cable Secondary Addresses window appears.

The secondary IP address enables CPE devices (hosts) attached to cable modem to talk to CMTS. (Usually this is a public IP address so that PCs can go to internet.)

**Figure 10-17** Cable Secondary Addresses



**Step 16** Enter an IP address in the IP address/Mask field and click **OK**. The MPLS Link Attribute Editor reappears.

**Step 17** Click **Next**. The MPLS Link Attribute Editor for the IP Address Scheme appears (see Figure 10-18).

**Figure 10-18** Specifying the MPLS Link IP Address Attributes

MPLS Link Attribute Editor - IP Address Scheme	
Attribute	Value
<b>PE-CE Interface Address/Mask</b>	
IP Numbering Scheme:	IP Numbered
PE Interface Address/Mask *:	10.1.3.1/24 (a.b.c.d/e)

Note: \* - Required Field

**Step 18** Edit any IP address scheme values that must be modified for this particular link, then click **Next**. The MPLS Link Attribute Editor for Routing Information appears (see Figure 10-19).

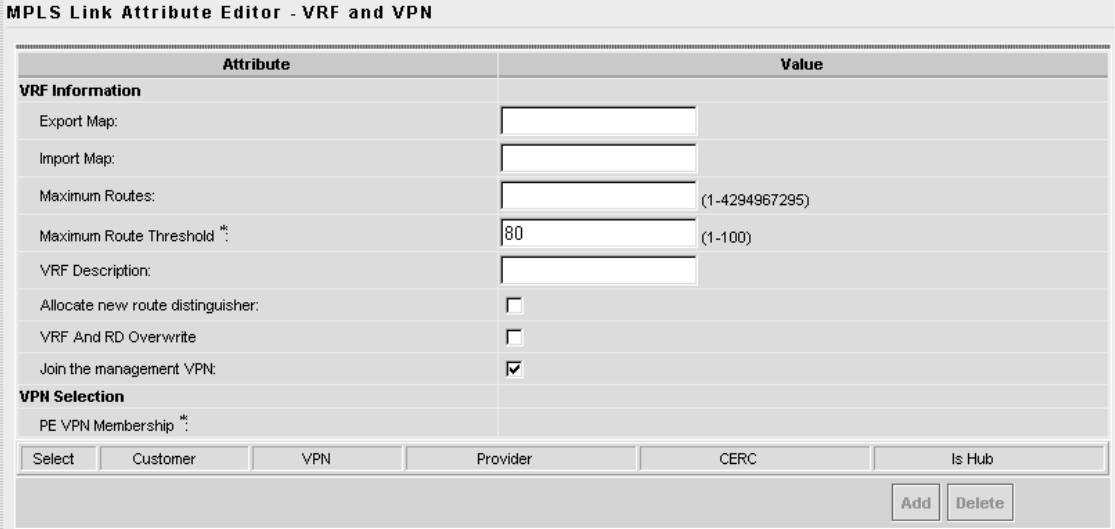
**Figure 10-19** Specifying the MPLS Link Routing Protocol Attributes

MPLS Link Attribute Editor - Routing Information	
Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	NONE
Redistribute Static (BGP only):	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input type="checkbox"/>

**Step 19** Edit any routing protocol values that must be modified for this particular link, then click **Next**.

The MPLS Link Attribute Editor for the VRF and VPN attributes appears (see Figure 10-20).

**Figure 10-20** Specifying the MPLS Link VRF and VPN Attributes



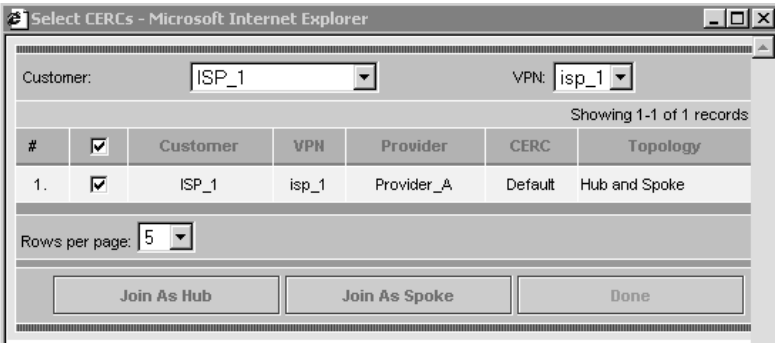
The dialog box is titled "MPLS Link Attribute Editor - VRF and VPN". It contains two main sections: "VRF Information" and "VPN Selection".

Attribute	Value
<b>VRF Information</b>	
Export Map:	<input type="text"/>
Import Map:	<input type="text"/>
Maximum Routes:	<input type="text"/> (1-4294967295)
Maximum Route Threshold *:	<input type="text"/> 80 (1-100)
VRF Description:	<input type="text"/>
Allocate new route distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite	<input type="checkbox"/>
Join the management VPN:	<input checked="" type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	<input type="text"/>
Select	Customer
VPN	Provider
CERC	Is Hub
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

The field values displayed in this dialog box reflect the values specified in the service policy associated with this service.

- Step 20** Check the check box for Join the Management VPN.
- Step 21** Edit any VRF and VPN values that must be modified for this particular link, then click **Add**. The Select CERCs/VPN dialog box appears.

**Figure 10-21** Choose CERCs



The dialog box is titled "Select CERCs - Microsoft Internet Explorer". It contains a form with "Customer:" and "VPN:" dropdown menus, both set to "ISP\_1". Below the form is a table showing 1-1 of 1 records.

#	<input checked="" type="checkbox"/>	Customer	VPN	Provider	CERC	Topology
1.	<input checked="" type="checkbox"/>	ISP_1	isp_1	Provider_A	Default	Hub and Spoke

Below the table is a "Rows per page:" dropdown set to "5". At the bottom are three buttons: "Join As Hub", "Join As Spoke", and "Done".

- Step 22** Choose the customer name and VPN.
- Step 23** Click **Join as Spoke**, then click **Done**.

The MPLS Link Attribute Editor for the VRF and VPN attributes appears (see Figure 10-22).

**Figure 10-22** Specifying the MPLS Link VRF and VPN Attributes

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value				
<b>VRF Information</b>					
Export Map:	<input type="text"/>				
Import Map:	<input type="text"/>				
Maximum Routes:	<input type="text"/> (1-4294967295)				
Maximum Route Threshold *:	<input type="text" value="80"/> (1-100)				
VRF Description:	<input type="text"/>				
Allocate new route distinguisher:	<input type="checkbox"/>				
VRF And RD Overwrite	<input type="checkbox"/>				
Join the management VPN:	<input checked="" type="checkbox"/>				
<b>VPN Selection</b>					
PE VPN Membership *:					
Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	ISP_1	isp_1	Provider_A	Default	<input type="checkbox"/>

Add Delete

95436

**Step 24** Edit any VRF and VPN values that must be modified for this particular link, then click **Next**.

You return to the MPLS Service Request Editor.

**Note**

You can define multiple links in this service request.

**Step 25** To save your work on this first link in the service request, click **Save**.

You return to the Service Requests dialog box, where the information for the link you just defined is now displayed.

**Figure 10-23** Service Request for an MPLS Link Completed

**MPLS Service Request Editor**

Job ID: SR ID: SR State:

Policy: cable1

Customer: Select Customer

Description:

Showing 1 - 1 of 1 record

#	<input type="checkbox"/>	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	<input type="checkbox"/>	0	Select CLE	<input type="text"/>	enpe1	Cable0/1	Edited	N/A

Rows per page:

Go to page:  of 1

Add Link Delete Link Save Cancel

126752

**Step 26** Click **Save**.





# Provisioning Carrier Supporting Carrier

This chapter describes how to configure the carrier supporting carrier (CSC) feature using the IP Solution Center (ISC) provisioning process. This chapter contains the following major sections:

- Carrier Supporting Carrier Overview, page 11-1
- Defining a CSC Service Policy, page 11-5
- Provisioning a CSC Service Request, page 11-5

## Carrier Supporting Carrier Overview

The carrier supporting carrier feature enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

This documentation focuses on a backbone carrier that offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services. There can be two types of customer carriers:

- An Internet service provider (ISP)
- A BGP/MPLS VPN service provider

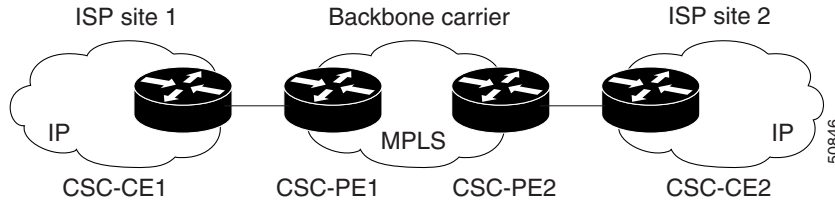
This documentation describes both types of customer carrier.

It is transparent to the backbone provider when either scenario is in use, after the required functionality for basic MPLS VPN CSC is implemented in the backbone network.

## Backbone Network with a Customer Carrier Who Is an ISP

In this network configuration, the customer carrier has two sites, each of which is a point of presence (POP). The customer carrier connects these sites using a VPN service provided by a backbone carrier, who uses MPLS. The ISP sites use IP. To enable packet transfer between the ISP sites and the backbone carrier, the CSC-CE routers that connect the ISPs to the backbone carrier run MPLS.

Figure 11-1 shows a carrier supporting carrier network configuration where the customer carrier is an ISP. The customer carrier has two sites, each of which is a point of presence (POP). The customer carrier connects these sites using a VPN service provided by the backbone carrier. The backbone carrier uses MPLS. The ISP sites use IP. To enable packet transfer between the ISP sites and the backbone carrier, the CSC-CE routers that connect the ISPs to the backbone carrier run MPLS.

**Figure 11-1** *Carrier Supporting Carrier Network with a Customer Carrier Who Is an ISP*

In this example, only the backbone carrier uses MPLS. The customer carrier (ISP) uses only IP. As a result, the backbone carrier must carry all the Internet routes of the customer carrier, which could be as many as 100,000 routes. This poses a scalability problem for the backbone carrier. To solve the scalability problem, the backbone carrier is configured as follows:

- The backbone carrier allows only internal routes of the customer carrier (IGP routes) to be exchanged between the CSC-CE routers of the customer carrier and the CSC-PE routers of the backbone carrier.
- MPLS is enabled on the interface between the CSC-CE router of the customer carrier and the CSC-PE router of the backbone carrier.

Internal and external routes are differentiated this way:

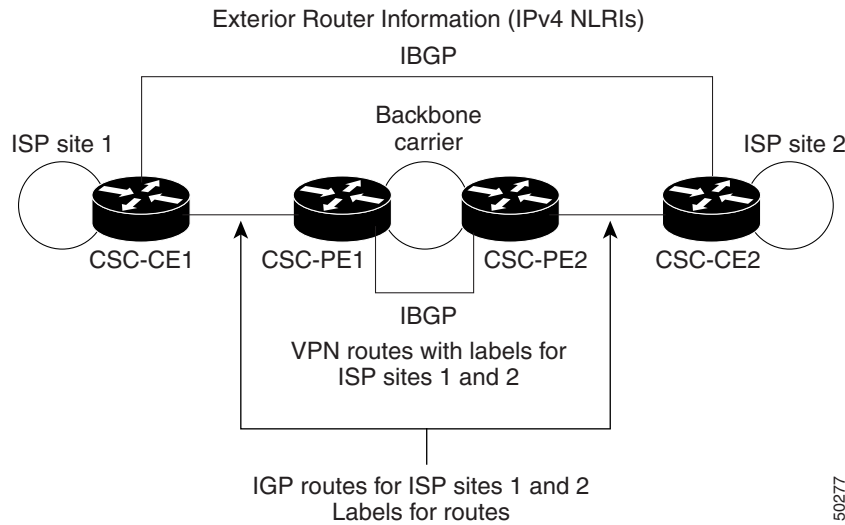
- Internal routes go to any of the routers within the ISP.
- External routes go to the Internet.

The number of internal routes is much smaller than the number of external routes. Restricting the routes between the CSC-CE routers of the customer carrier and the CSC-PE routers of the backbone carrier significantly reduces the number of routes that the CSC-PE router needs to maintain.

Since the CSC-PE routers do not have to carry external routes in the VRF routing table, they can use the incoming label in the packet to forward the customer carrier Internet traffic. Adding MPLS to the routers provides a consistent method of transporting packets from the customer carrier to the backbone carrier. MPLS allows the exchange of an MPLS label between the CSC-PE and the CSC-CE routers for every internal customer carrier route. The routers in the customer carrier have all the external routes either through IBGP or route redistribution to provide Internet connectivity.

Figure 11-2 shows how information is exchanged when the network is configured in this manner.

**Figure 11-2** Backbone Carrier Exchanging Routing Information with a Customer Carrier Who Is an ISP



50277

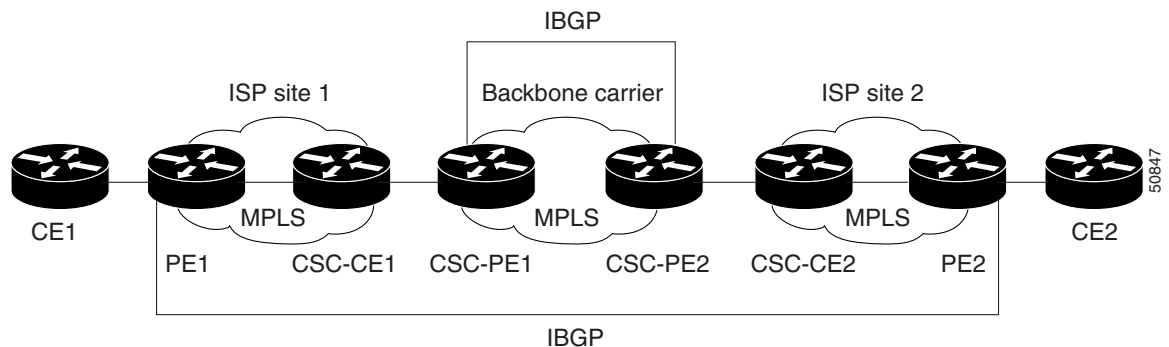
## Backbone Network with a Customer Carrier Who Is a BGP/MPLS VPN Service Provider

When a backbone carrier and the customer carrier both provide BGP/MPLS VPN services, the method of transporting data is different from when a customer carrier provides only ISP services. The following list highlights those differences.

- When a customer carrier provides BGP/MPLS VPN services, its external routes are VPN-IPv4 routes. When a customer carrier is an ISP, its external routes are IP routes.
- When a customer carrier provides BGP/MPLS VPN services, every site within the customer carrier must use MPLS. When a customer carrier is an ISP, the sites do not need to use MPLS.

Figure 11-3 figure shows a carrier supporting carrier network configuration where the customer carrier is an MPLS VPN provider. The customer carrier has two sites. The backbone carrier and the customer carrier use MPLS. The IBGP sessions exchange the external routing information of the ISP.

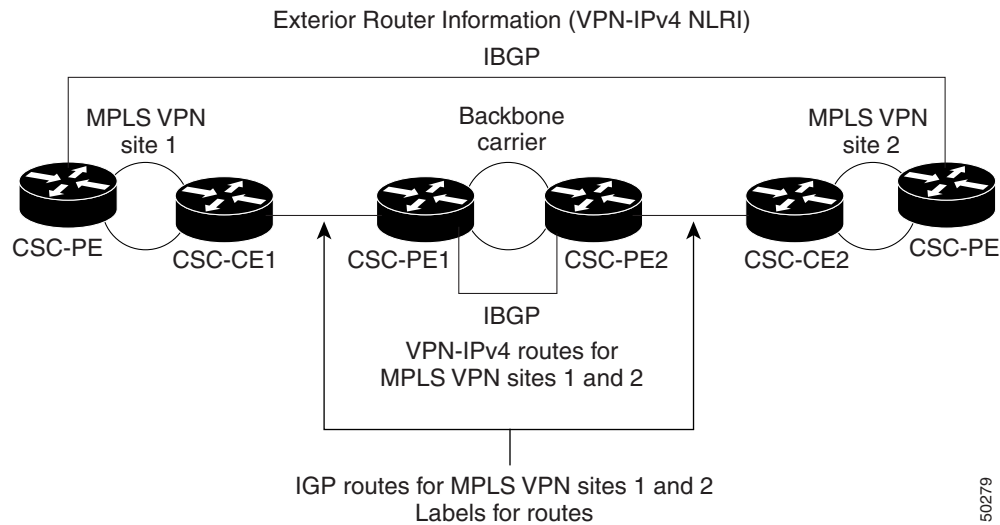
**Figure 11-3** Carrier Supporting Carrier Network with a Customer Carrier Who Is an MPLS VPN Provider



50847

Figure 11-3 figure shows exchanging information with a customer carrier who is an MPLS VPN service provider.

**Figure 11-4** *Backbone Carrier Exchanging Information with a Customer Carrier Who Is an MPLS VPN Service Provider*



## ISC Configuration Options

To configure the CSC network to exchange routes and carry labels between the backbone carrier provider edge (CSC-PE) routers and the customer carrier customer edge (CSC-CE) routers, use Label Distribution Protocol (LDP) to carry the labels and an Internal Gateway Protocol (IGP) to carry the routes.

### LDP/IGP

A routing protocol is required between the CSC-PE and CSC-CE routers that connect the backbone carrier to the customer carrier. The routing protocol enables the customer carrier to exchange IGP routing information with the backbone carrier. RIP, OSPF, or static routing as the routing protocol can be selected.

Label distribution protocol (LDP) is required between the CSC-PE and CSC-CE routers that connect the backbone carrier to the customer carrier. LDP is also required on the CSC-PE to CSC-CE interface for VPN routing/forwarding (VRF).

### IPv4 BGP Label Distribution

BGP takes the place of an IGP and LDP in a VPN forwarding/routing instance (VRF) table. You can use BGP to distribute routes and MPLS labels. Using a single protocol instead of two simplifies the configuration and troubleshooting.

BGP is the preferred routing protocol for connecting two ISPs, mainly because of its routing policies and ability to scale. ISPs commonly use BGP between two providers. This feature enables those ISPs to use BGP.

When BGP (both EBGp and IBGP) distributes a route, it can also distribute an MPLS label that is mapped to that route. The MPLS label mapping information for the route is carried in the BGP update message that contains the information about the route. If the next hop is not changed, the label is preserved.

## Defining a CSC Service Policy

To define a Service Policy with CSC, choose the CSC Support check box from the MPLS Policy Editor - Routing Information, as shown in Figure 11-5.

**Figure 11-5** CSC Service Policy

**MPLS Policy Editor - Routing Information**

Attribute	Value	Editable
<b>PE-CE Routing Information</b>		
Routing Protocol	RIP	<input checked="" type="checkbox"/>
CsC Support:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RIP Metrics (BGP only):	<input type="text"/> (1-16)	<input checked="" type="checkbox"/>
Redistributed Protocols on PE	<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>
Redistributed Protocols on CE:	<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>

101888

When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service.

## Provisioning a CSC Service Request

To provision a Service Request with CSC, choose the CSC Support check box from the MPLS Link Attribute Editor - Routing Information, as shown in Figure 11-6.

Figure 11-6 CSC Service Request

**MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	RIP
CsC Support:	<input checked="" type="checkbox"/>
Give Only Default Routes to CE:	<input type="checkbox"/>
Redistribute Static (BGP only):	<input type="checkbox"/>
Redistribute Connected (BGP only):	<input checked="" type="checkbox"/>
RIP Metrics (BGP only):	<input type="text"/> (1-16)
Redistributed Protocols on PE	<input type="button" value="Edit"/>
Redistributed Protocols on CE:	<input type="button" value="Edit"/>

101889

When CSC Support is checked, the CSC functionality is enabled for the MPLS VPN service.



## Provisioning Multiple Devices

---

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

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

### NPC Ring Topology

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

This section contains the following sections:

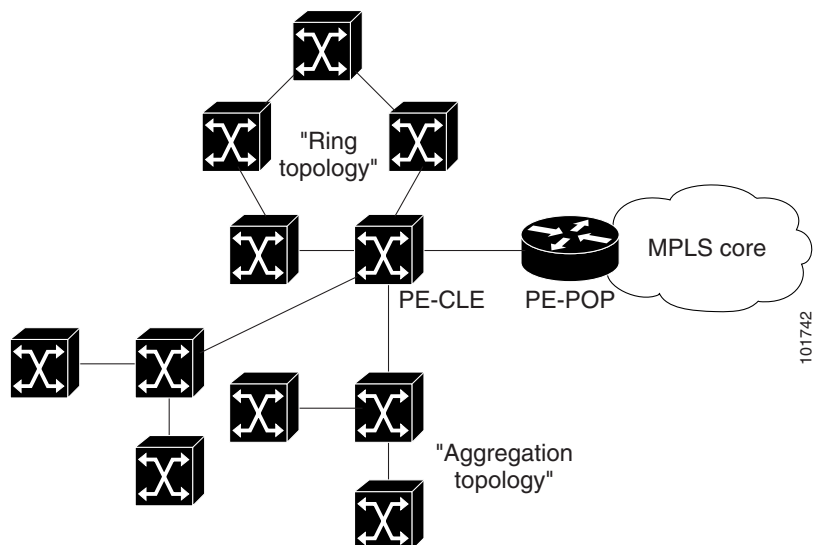
- Ring Topology Overview, page 12-1
- Creating a Ring of Three PE-CLE, page 12-2
- Configuring NPC Ring Topology, page 12-4

### Ring Topology Overview

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

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

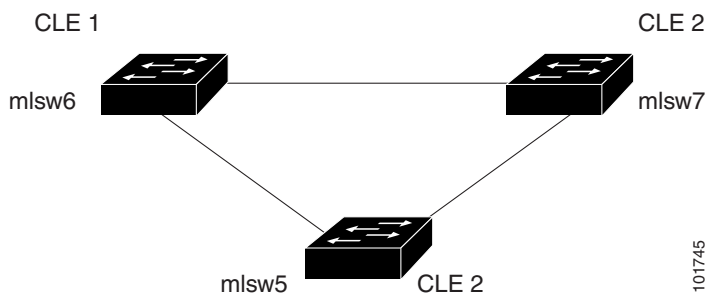
Figure 12-1 shows an example of these two basic L2 access topologies.

**Figure 12-1** L2 Access Topologies

## Creating a Ring of Three PE-CLE

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

Figure 12-2 shows an example ring of three Catalyst 3550 switches: mls w5, mls w6, and mls w7.

**Figure 12-2** A Ring of Three PE-CLE

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

- 
- Step 1** Log in to ISC.
  - Step 2** Go to **Service Inventory > Inventory and Connection Manager**.
  - Step 3** Click **NPC Rings** in the TOC under **Named Physical Circuits**.

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

**Figure 12-3 NPC Rings**

NPC Rings

Show NPC rings with name matching

Showing 0 of 0 records

#	Name
Rows per page: 10	

Go to page: 1 of 0

**Step 4** Click **Create** to continue.

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

**Figure 12-4 Create Ring**

Create Ring

#	Source Device	Source Interface	Destination Device	Destination Interface
1.	<input type="checkbox"/> Select source device	Select source interface	Select destination device	Select destination interface
2.	<input type="checkbox"/> Select source device	Select source interface	Select destination device	Select destination interface
3.	<input type="checkbox"/> Select source device	Select source interface	Select destination device	Select destination interface

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

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

**Note**

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

**Figure 12-5 Show Devices**

Show  devices where  matching

Showing 1-1 of 1 records

#	Select	Device Name	Provider Name	Region Name	PE Role Type
1.	<input checked="" type="radio"/>	mlsw6.cisco.com	PROVIDER-X	NORTH-X	PE_CLE

Rows per page: All

Go to page: 1 of 1

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

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

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

**Figure 12-6 Create Ring**

#	Source Device	Source Interface	Destination Device	Destination Interface
1.	<input type="checkbox"/> mls w6	FastEthernet0/3	mlsw7	FastEthernet0/3
2.	<input type="checkbox"/> mls w7	FastEthernet0/2	mlsw5	FastEthernet0/4
3.	<input type="checkbox"/> mls w5	FastEthernet0/3	mlsw6	FastEthernet0/2

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



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

- Step 9** Click **Save** to save your ring in the Repository.  
The NPC Rings window appears, as shown in Figure 12-7

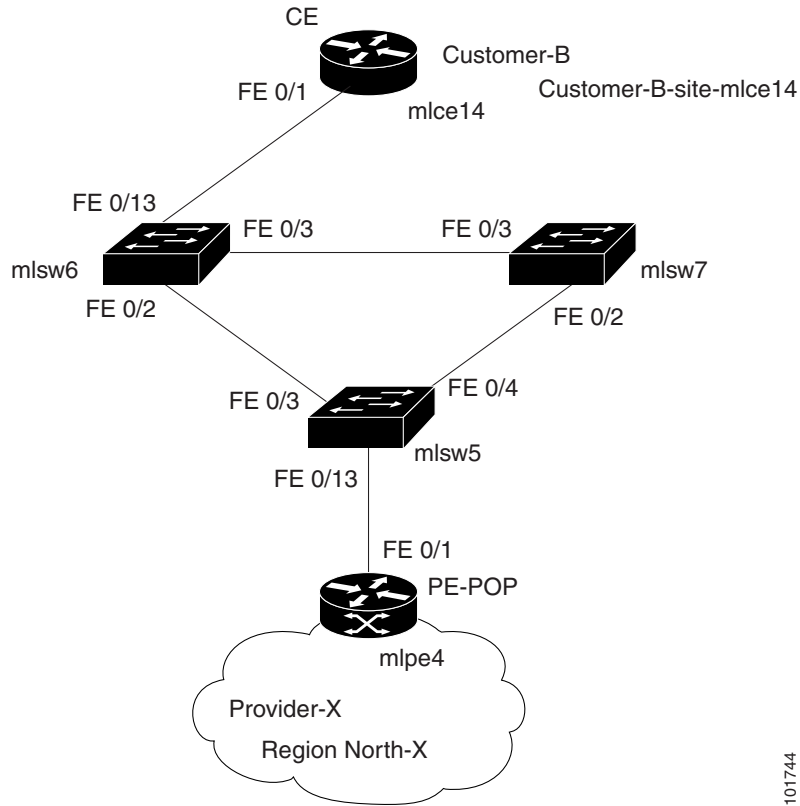
**Figure 12-7 NPC Rings**

NPC Rings	
Show NPC rings with name matching <input type="text"/> <input type="button" value="Find"/>	
Showing 1 - 1 of 1 record	
#	Name
1.	<input type="checkbox"/> 1-mlsw6-FastEthernet0/3
Rows per page: <input type="text" value="10"/> Go to page: <input type="text" value="1"/> of 1 <input type="button" value="Go"/>	
<input type="button" value="Create"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

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

## Configuring NPC Ring Topology

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

**Figure 12-8 The Ring Topology**

101744

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

- Step 1** Log in to ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Named Physical Circuits**. The Named Physical Circuits window appears, as shown in Figure 12-9.

**Figure 12-9 Named Physical Circuits**

The screenshot shows the "Named Physical Circuits" window. It includes a search bar with "Show NPCs where" and a dropdown menu set to "Name". There is a "Find" button. Below the search bar, it says "Showing 0 of 0 records". A table with columns: #, Source Device, Source Interface, Destination Device, Destination Interface, and Name is visible. Below the table, there is a "Rows per page" dropdown set to "10" and a "Go to page" field set to "1" of "1". There are "Create" and "Delete" buttons at the bottom right.

116324

- Step 3** Click **Create**. The Create Named Physical Circuits window appears, as shown in Figure 12-10.

**Figure 12-10** Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
---	--------	--------------------	--------------------	------

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

**Step 4** Click **Add Device**.

The Select Devices window appears (not shown).

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

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

**Figure 12-11** Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	<input checked="" type="checkbox"/> mlce14			

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

**Step 6** Click **Add Device**.

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

**Figure 12-12** Choose Devices

Show **PE** devices where **Device Name** Matching \* Find

Showing 1 - 7 of 7 records

#	Device Name	Provider Name	Region Name	PE Role Type
1.	<input type="radio"/> mlpe1	Provider-X	West-X	PE_POP
2.	<input type="radio"/> mlpe2	Provider-X	West-X	PE_POP
3.	<input type="radio"/> mlpe3	Provider-X	West-X	PE_POP
4.	<input checked="" type="radio"/> mlpe4	Provider-X	West-X	PE_POP
5.	<input type="radio"/> mlsw5	Provider-X	North-X	PE_CLE
6.	<input type="radio"/> mlsw6	Provider-X	North-X	PE_CLE
7.	<input type="radio"/> mlsw7	Provider-X	North-X	PE_CLE

Rows per page: 50 Go to page: 1 of 1 Select Cancel

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

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

**Figure 12-13** Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	<input checked="" type="checkbox"/> mlce14		Select outgoing interface	
2.	<input type="checkbox"/> mlpe4	Select incoming interface		

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

**Step 8** Click **Insert Ring**.

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

**Figure 12-14** Create a Named Physical Circuit

Show NPC rings with Ring Name Matching \* Find

Showing 1 - 1 of 1 record

#	Ring Name
1.	<input checked="" type="radio"/> 1-mlsw6-FastEthernet0/3

Rows per page: 10 Go to page: 1 of 1

Select Cancel

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

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

**Figure 12-15** Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	<input type="checkbox"/> mlce14		Select outgoing interface	
2.	<input checked="" type="checkbox"/> Select device	Select incoming interface		1-mlsw6-FastEthernet0/3
3.	<input type="checkbox"/> Select device		Select outgoing interface	1-mlsw6-FastEthernet0/3
4.	<input type="checkbox"/> mlpe4	Select incoming interface		

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

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

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

**Figure 12-16 Show PE Devices**

Showing 1 - 3 of 3 records

#	Device Name	Provider Name	Region Name	PE Role Type
1.	<input type="radio"/> mls5	Provider-X	North-X	PE_CLE
2.	<input checked="" type="radio"/> mls6	Provider-X	North-X	PE_CLE
3.	<input type="radio"/> mls7	Provider-X	North-X	PE_CLE

Rows per page: 10 Go to page: 1 of 1

Select Cancel

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

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

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

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

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

**Figure 12-17 Create a Named Physical Circuit**

Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	<input checked="" type="checkbox"/> mlce14		FastEthernet0/1	
2.	<input type="checkbox"/> mls6	FastEthernet0/13		1-mls6-FastEthernet0/3
3.	<input type="checkbox"/> mls5		FastEthernet0/13	1-mls6-FastEthernet0/3
4.	<input type="checkbox"/> mlpe4	FastEthernet0/1		

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

**Step 14** Click **Save**.

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

**Figure 12-18**     **Named Physical Circuits**

Named Physical Circuits

Show NPCs where  Matching

Showing 1 - 4 of 4 records

#	<input type="checkbox"/>	Source Device	Source Interface	Destination Device	Destination Interface	Name
1.	<input type="checkbox"/>	mlsw5	FastEthernet0/13	mlpe4	FastEthernet0/1	1-(mlsw5-FastEthernet0/13) <==>(mlpe4-FastEthernet0/1)
2.	<input type="checkbox"/>	mlsw6		mlpe4	FastEthernet0/1	2-(mlsw6-)<==> (mlpe4-FastEthernet0/1)
3.	<input type="checkbox"/>	mlsw7		mlpe4	FastEthernet0/1	3-(mlsw7-)<==> (mlpe4-FastEthernet0/1)
4.	<input type="checkbox"/>	mlce14	FastEthernet0/1	mlpe4	FastEthernet0/1	4-(mlce14-FastEthernet0/1) <==>(mlpe4-FastEthernet0/1)

Rows per page:

Go to page:  of 1

116336

## Ethernet-To-The-Home

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

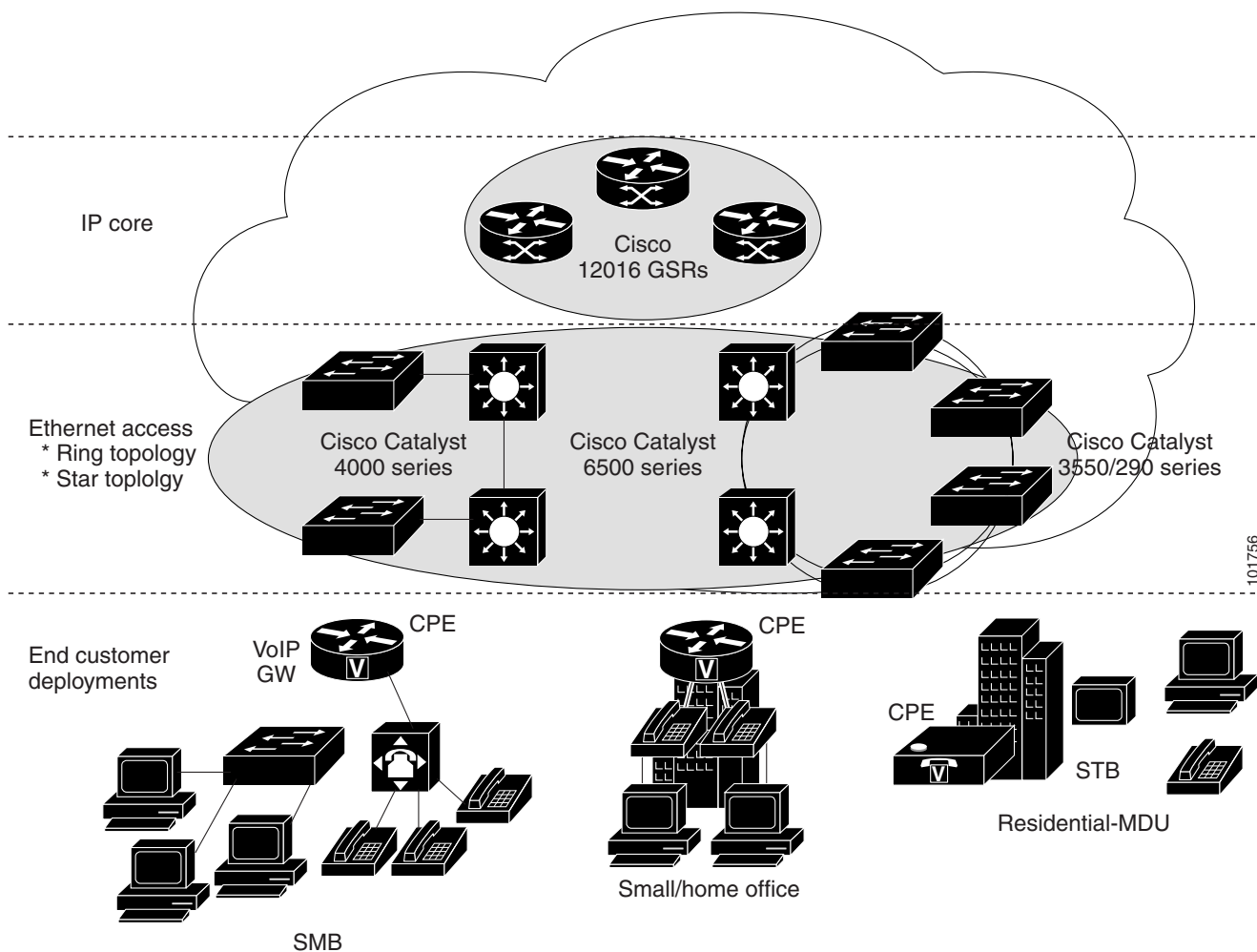
- ETTH Overview, page 12-9
- Configuring ETTH, page 12-11
- Residential Service, page 12-15

### ETTH Overview

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

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

Figure 12-19 Cisco ETTx Solution



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

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

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

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

## Access Domain Management

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

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

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

## ISC ETTH Implementation

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

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

### PVLAN or Protected Port

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

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

### Access Port

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

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

### IGMP with MVR

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

## Configuring ETTH

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

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Log in to ISC.  |
| <b>Step 2</b> | Go to <b>Service Design &gt; Policies</b> .                               |
| <b>Step 3</b> | From the Policies window, choose a Service Policy and click <b>Edit</b> . |

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

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

**Figure 12-20 MPLS Policy Editor - Interface**

Attribute	Value	Editable
<b>Reset all Attribute editable flags:</b>		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Auto-Pick VLAN ID:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Link Speed:	None	<input checked="" type="checkbox"/>
Link Duplex:	None	<input checked="" type="checkbox"/>
ETTH Support:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>CE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>

Step 2 of 5 -

< Back Next > Finish Cancel

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

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

**Figure 12-21 ETTH UNI Information**

Attribute	Value	Editable
ETTH Support:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Information</b>		
Private VLAN/Protected Port:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IGMP Snooping with MVR:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>CE Information</b>		

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

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

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

**Figure 12-22** *ETTH UNI Information Options*

UNI Information		
Private VLAN/Protected Port:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IGMP Snooping with MVR:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mode:	<input checked="" type="radio"/> Compatible <input type="radio"/> Dynamic	<input checked="" type="checkbox"/>
Query Time:	<input type="text" value=""/> (1-100)	<input checked="" type="checkbox"/>
Immediate:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

101747

**Step 8** Choose UNI Information options:

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

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

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

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

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

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

**Figure 12-23 MPLS Link Attribute Editor - Interface**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>PE Information</b>	
PE	enswosr1
Interface Name:	GE-WAN9/2. <input type="text"/>
Interface Description:	<input type="text"/>
Shutdown Interface:	<input type="checkbox"/>
CE Encapsulation: ⓘ	DOT1Q ▾
Auto-Pick VLAN ID:	<input checked="" type="checkbox"/>
Link Speed:	None ▾
Link Duplex:	None ▾
ETTH Support:	<input checked="" type="checkbox"/>
<b>UNI Information</b>	
Private VLAN/Protected Port:	<input checked="" type="checkbox"/>
Secondary VLAN ID: ⓘ	567 (1-4094)
IGMP Snooping with MVR:	<input checked="" type="checkbox"/>
Mode:	<input checked="" type="radio"/> Compatible <input type="radio"/> Dynamic
Query Time:	80 (1-100)
Multicast IP Address:	<input type="button" value="Edit"/>
Multicast VLAN ID:	888 (1-4094)
Immediate:	<input checked="" type="checkbox"/>

Note: \* - Required Field

- Step 1 of 4 -

< Back Next > Finish Cancel

101750

**Step 13** Edit the following Link Attribute specific UNI Information:

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

**Step 14** Click **EDIT**.

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

**Figure 12-24** Multicast IP Addresses

Multicast IP Addresses		
Select	Multicast IP Address (a.b.c.d)	Counter (1 - 256)
<input type="checkbox"/>	224.3.3.1	12

101751

Add Delete OK Cancel

**Step 15** Edit the following Link Attribute specific UNI Information:

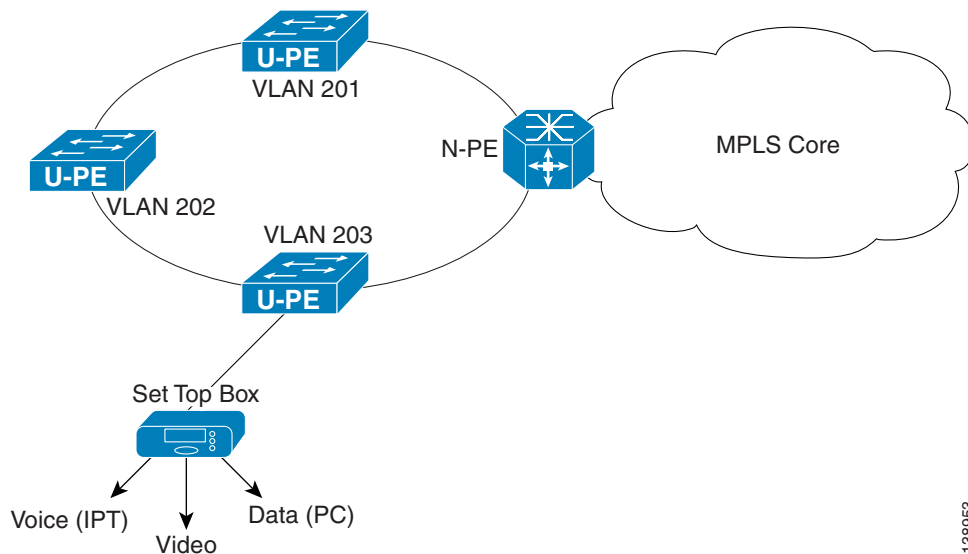
- **Multicast IP Address**—Enter an *IP Address* for the join the multicast group, which allows users to have access to video on demand, for example.
- **Counter**—Enter a *count* to determine the number of contiguous IP addresses starting with the Multicast IP Address.

**Step 16** Click **OK**.

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

## Residential Service

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

**Figure 12-25** Residential Services

# Policy for Residential Services Over Shared VLAN

A special policy must e created by enabling Shared VLAN.

- Step 1** Log in to ISC.
- Step 2** Go to **Service Design > Policies**.
- Step 3** From the Policies window, click **Create > MPLS Policy**.  
The Policy Type window appears (see Figure 12-26).

Figure 12-26 Policy Type

MPLS Policy Editor - Policy Type

Attribute	Value
Policy Name *	mlResServ1
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Policy Type:	<input checked="" type="radio"/> Regular: PE-CE <input type="radio"/> MVRFC: PE-CE
CE Present:	<input type="checkbox"/>

Note: \* - Required Field

- Step 4** In the Policy Name field, enter a policy name.
- Step 5** Under Policy Owner, click the **Global Policy** radio button.
- Step 6** Under Policy Type accept **Regular: PE-CE**.
- Step 7** Under CE Present, uncheck the check box, then click **Next**.  
The MPLS Policy Editor - Interface window appears (see Figure 12-27).

**Figure 12-27**     *Interface Settings*

**MPLS Policy Editor - Interface**

Attribute	Value	Editable
<b>Reset All Attribute Editable Flags:</b>		<input checked="" type="checkbox"/>
<b>PE Information</b>		
Interface Type:	ANY	
Interface Format:		
Interface Description:		<input checked="" type="checkbox"/>
Shutdown Interface:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Auto-Pick VLAN ID:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use SVI:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Link Speed:	None	<input checked="" type="checkbox"/>
Link Duplex:	None	<input checked="" type="checkbox"/>
ETTH Support:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Standard UNI Port:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Information</b>		
Shared VLAN:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Private VLAN/Protected Port:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IGMP Snooping with MVR:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Security Information</b>		
Disable CDP:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Filter BPDU:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use Existing ACL Name:	<input type="checkbox"/>	
UNI MAC Addresses:	Edit	<input checked="" type="checkbox"/>
UNI Port Security:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- Step 8** Check the **Use SVI:** check box, then wait for the screen to refresh.
- Step 9** Check the **ETTH Support:** check box, then wait for the screen to refresh.
- Step 10** Check the **Standard UNI Port:** check box, then wait for the screen to refresh.
- Step 11** Check the **Shared VLAN:** check box, then wait for the screen to refresh.
- Some fields are now grayed-out.



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

- Step 12** Check the **Private VLAN/Protected Port:** check box, wait for the screen to refresh, then click **Next**.
- Step 13** In the IP Address Scheme window, you can continue by clicking **Next**.
- Step 14** In the Routing Information window, you can continue by clicking **Next**.
- Step 15** In the VRF and VPN Member window, you can finish creating this policy by clicking **Finish**.

## Service Requests

- Step 1** Log in to ISC.
- Step 2** Go to **Service Inventory > Inventory and Connection Manager > Service Requests**.

- Step 3** From the Service Requests window, click **Create > MPLS VPN**.  
The Select MPLS Policy window appears.
- Step 4** Choose the policy you configured for Shared VLAN Residential Services, then click **OK**.  
The MPLS Service Request Editor window appears.
- Step 5** In the MPLS Service Request Editor window, click **Add Link**, then wait for the window to refresh.
- Step 6** Click the active field **Select U-PE**.
- Step 7** Choose a PE device, then click **Select**.
- Step 8** From the active drop-down list, choose an interface, then wait for the window to refresh.
- Step 9** Under Link Attributes column, click the active **Add** field.  
The Interface window appears (see Figure 12-28).



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

**Figure 12-28 Interface Attributes**

**MPLS Link Attribute Editor - Interface**

Attribute	Value
<b>PE Information</b>	
PE	mlpe5
Interface Name:	FastEthernet8/25. (1-4294967295)
Interface Description:	
Shutdown Interface:	<input type="checkbox"/>
CE Encapsulation:	DOT1Q
VLAN ID *	55 (1-4095)
Auto-Pick VLAN ID:	<input type="checkbox"/>
Use SVI:	<input checked="" type="checkbox"/>
Link Speed:	None
Link Duplex:	None
ETTH Support:	<input checked="" type="checkbox"/>
Standard UNI Port:	<input checked="" type="checkbox"/>
<b>UNI Information</b>	
Shared VLAN:	<input checked="" type="checkbox"/>
Private VLAN/Protected Port:	<input checked="" type="checkbox"/>
Secondary VLAN ID:	(1-4094)
IGMP Snooping with MVR:	<input type="checkbox"/>
<b>UNI Security Information</b>	
Disable CDP:	<input type="checkbox"/>
Filter BPDU:	<input type="checkbox"/>
Use Existing ACL Name:	<input type="checkbox"/>
UNI MAC Addresses:	Edit
UNI Port Security:	<input type="checkbox"/>

Note: \* - Required Field

- Step 10** Enter a valid **VLAN ID** value, then click **Next**.  
The IP Address Scheme window appears (see Figure 12-29).

**Figure 12-29** Entering IP Address Scheme

**MPLS Link Attribute Editor - IP Address Scheme**

Attribute	Value
<b>PE-CE Interface Address/Mask</b>	
IP Numbering Scheme:	IP Numbered ▾
Automatically Assign IP Addresses:	<input type="checkbox"/>
PE Interface Address/Mask *:	<input type="text"/> (a.b.c.d/e)
Secondary IP Address/Mask - 1 *:	<input type="text"/> (a.b.c.d/e)
Secondary IP Address/Mask - 2 *:	<input type="text"/> (a.b.c.d/e)
DHCP Helper IP Address *:	<input type="text"/> (a.b.c.d)

Note: \* - Required Field

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

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

**Figure 12-30** Selecting Routing Information

**MPLS Link Attribute Editor - Routing Information**

Attribute	Value
<b>PE-CE Routing Information</b>	
Routing Protocol	NONE ▾
CsC Support:	<input type="checkbox"/>
Redistribute Static (BGP only):	<input checked="" type="checkbox"/>
Redistribute Connected (BGP only):	<input checked="" type="checkbox"/>

Note: \* - Required Field

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

**Figure 12-31** Selecting VRF and VPN Attributes

**MPLS Link Attribute Editor - VRF and VPN**

Attribute	Value
<b>VRF Information</b>	
Export Map:	<input type="text"/>
Import Map:	<input type="text"/>
Maximum Routes:	<input type="text"/> (1-4294967295)
Maximum Route Threshold *:	80 (1-100)
VRF Description:	<input type="text"/>
Allocate New Route Distinguisher:	<input type="checkbox"/>
VRF And RD Overwrite:	<input type="checkbox"/>
<b>VPN Selection</b>	
PE VPN Membership *:	
Select	Customer
<input type="checkbox"/>	LuanCustomer
VPN	LuanVPN1
Provider	LuanProvider
CERC	LuanCERC1
Is Hub	<input checked="" type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

Note: \* - Required Field

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

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

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

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

---



# Spanning Multiple Autonomous Systems

This chapter describes how to configure spanning multiple autonomous systems using the IP Solution Center (ISC) provisioning process. This chapter contains the following major sections:

- Overview, page 13-1
- Routing Between Autonomous Systems, page 13-2
- Routing Between Subautonomous Systems in a Confederation, page 13-8
- Using ISC to Span Multiple Autonomous Systems, page 13-10

## Overview

The inter-autonomous system for MPLS VPNs feature allows an MPLS VPN to span service providers and autonomous systems. An autonomous system is a single network or group of networks that is controlled by a common system administration group and that uses a single, clearly defined routing protocol.

As VPNs grow, their requirements expand. In some cases, VPNs need to reside on different autonomous systems in different geographic areas. Also, some VPNs need to extend across multiple service providers (overlapping VPNs). Regardless of the complexity and location of the VPNs, the connection between autonomous systems must be seamless to the customer.

The inter-autonomous systems for MPLS VPNs feature provides that seamless integration of autonomous systems and service providers. Separate autonomous systems from different service providers can communicate by exchanging IPv4 network layer reachability information (NLRI) in the form of VPN-IPv4 addresses. The autonomous systems' border edge routers use the Exterior Border Gateway Protocol (EBGP) to exchange that information. An interior gateway protocol (IGP) then distributes the network layer information for VPN-IPv4 prefixes throughout each VPN and each autonomous system. Routing information uses the following protocols:

- Within an autonomous system, routing information is shared using an interior gateway protocol.
- Between autonomous systems, routing information is shared using an Exterior Border Gateway Protocol. An EBGp allows a service provider to set up an inter-domain routing system that guarantees the loop-free exchange of routing information between separate autonomous systems.

An MPLS VPN with inter-autonomous system support allows a service provider to provide to customers scalable Layer 3 VPN services, such as web hosting, application hosting, interactive learning, electronic commerce, and telephony service. A VPN service provider supplies a secure, IP-based network that shares resources on one or more physical networks.

The primary function of EBGp is to exchange network reachability information between autonomous systems, including information about the list of autonomous system routes. The autonomous systems use EBGp border edge routers to distribute the routes, which include label switching information. Each border edge router rewrites the next-hop and MPLS labels. See *Routing Between Autonomous Systems*, page 13-2 for more information.

Inter-autonomous system configurations supported in an MPLS VPN can include:

- *Interprovider VPN*: MPLS VPNs that include two or more autonomous systems, connected by separate border edge routers. The autonomous systems exchange routes using EBGp. No interior gateway protocol (IGP) or routing information is exchanged between the autonomous systems.
- *BGP Confederations*: MPLS VPNs that divide a single autonomous system into multiple sub-autonomous systems, and classify them as a single, designated confederation. The network recognizes the confederation as a single autonomous system. The peers in the different autonomous systems communicate over EBGp sessions; however, they can exchange route information as if they were IBGP peers.

## Benefits

The inter-autonomous system MPLS VPN feature provides the following benefits:

- Allows a VPN to cross more than one service provider backbone

The inter-autonomous systems for MPLS VPNs feature allows service providers, running separate autonomous systems, to jointly offer MPLS VPN services to the same end customer. A VPN can begin at one customer site and traverse different VPN service provider backbones before arriving at another site of the same customer. Previously, MPLS VPNs could only traverse a single BGP autonomous system service provider backbone. The inter-autonomous system feature allows multiple autonomous systems to form a continuous (and seamless) network between a service provider's customer sites.

- Allows a VPN to exist in different areas

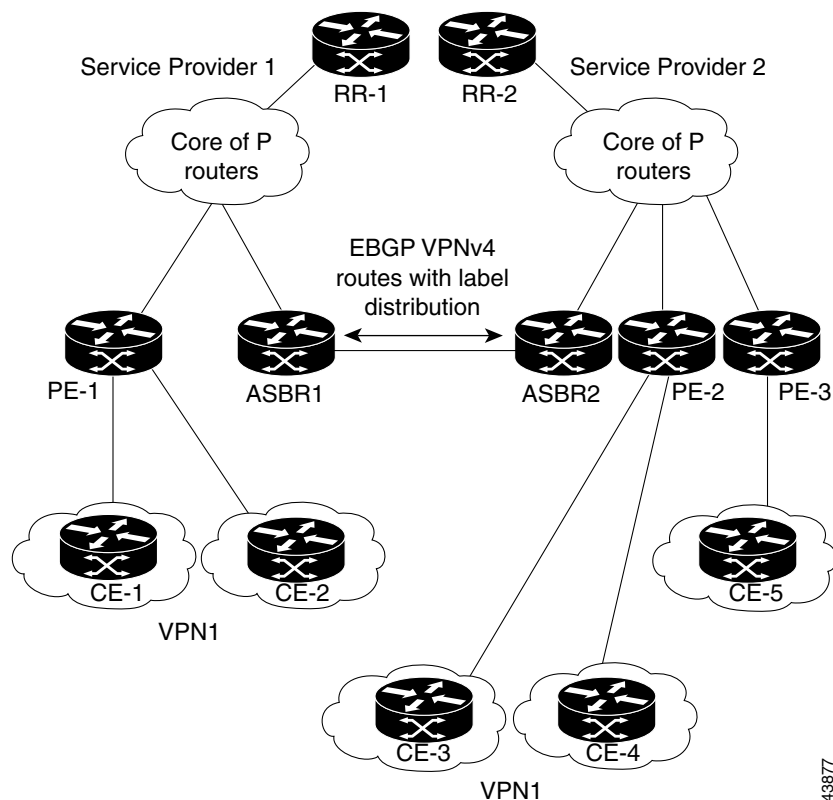
The inter-autonomous systems for MPLS VPNs feature allows a service provider to create a VPN in different geographic areas. Having all VPN traffic flow through one point (between the areas) allows for better rate control of network traffic between the areas.

- Allows confederations to optimize IBGP meshing

The inter-autonomous systems feature can make IBGP meshing in an autonomous system more organized and manageable. You can divide an autonomous system into multiple, separate sub-autonomous systems and then classify them into a single confederation (even though the entire VPN backbone appears as a single autonomous system). This capability allows a service provider to offer MPLS VPNs across the confederation because it supports the exchange of labeled VPN-IPv4 network layer reachability information between the sub-autonomous systems that form the confederation.

## Routing Between Autonomous Systems

Figure 13-1 illustrates one MPLS VPN consisting of two separate autonomous systems. Each autonomous system operates under different administrative control and runs a different IGP. Service providers exchange routing information through EBGp border edge routers (ASBR1 and ASBR2).

**Figure 13-1** *EBGP Connection Between Two Autonomous Systems*

This configuration uses the following process to transmit information:

1. The provider edge router (PE-1) assigns a label for a route before distributing that route. The PE router uses the multiprotocol extensions of a border gateway protocol (BGP) to transmit label mapping information. The PE router distributes the route as a VPN-IPv4 address. The address label and the VPN identifier are encoded as part of the NLRI.
2. The two route reflectors (RR-1 and RR-2) reflect VPN-IPv4 internal routes within the autonomous system. The autonomous systems' border edge routers (ASBR1 and ASBR2) advertise the VPN-IPv4 external routes.
3. The EBGP border edge router (ASBR1) redistributes the route to the next autonomous system, (ASBR2). ASBR1 specifies its own address as the value of the EBGP next hop attribute and assigns a new label. The ASBR1 address ensures the following:
  - The next hop router is always reachable in the service provider (P) backbone network.
  - The label assigned by the distributing router is properly interpreted. The label associated with a route must be assigned by the corresponding next hop router.
4. The EBGP border edge router (ASBR2) redistributes the route in one of the following ways, depending on its configuration:
  - If the IBGP neighbors are configured with the **neighbor next-hop-self** command, ASBR2 changes the next hop address of updates received from the EBGP peer, then forwards it on.
  - If the IBGP neighbors are not configured with the **neighbor next-hop-self** command, the next hop address does not get changed. ASBR2 must propagate a host route for the EBGP peer through the IGP.

To propagate the EBGp VPN-IPv4 neighbor host route, use the **redistribute connected subnets** command. The EBGp VPN-IPv4 neighbor host route is automatically installed in the routing table when the neighbor comes up. This is essential to establish the label-switched path between PE routers in different autonomous systems.

## Exchanging VPN Routing Information

Autonomous systems exchange VPN routing information (routes and labels) to establish connections. To control connections between autonomous systems, the PE routers and EBGp border edge routers maintain a Label Forwarding Information Base (LFIB). The LFIB manages the labels and routes that the PE routers and EBGp border edge routers receive during the exchange of VPN information.

Figure 13-2 illustrates the exchange of VPN route and label information between autonomous systems. The autonomous systems use the following guidelines to exchange VPN routing information:

*Routing information* includes:

- The destination network (N)
- The next hop field associated with the distributing router
- A local MPLS label (L)

An *RD1: route distinguisher* is part of a destination network address to make the VPN-IPv4 route globally unique in the VPN service provider environment.

The *ASBRs* are configured to change the next hop (next-hop-self) when sending VPN-IPv4 NLRI to the IBGP neighbors. Therefore, the ASBRs must allocate a new label when they forward the NLRI to the IBGP neighbors.

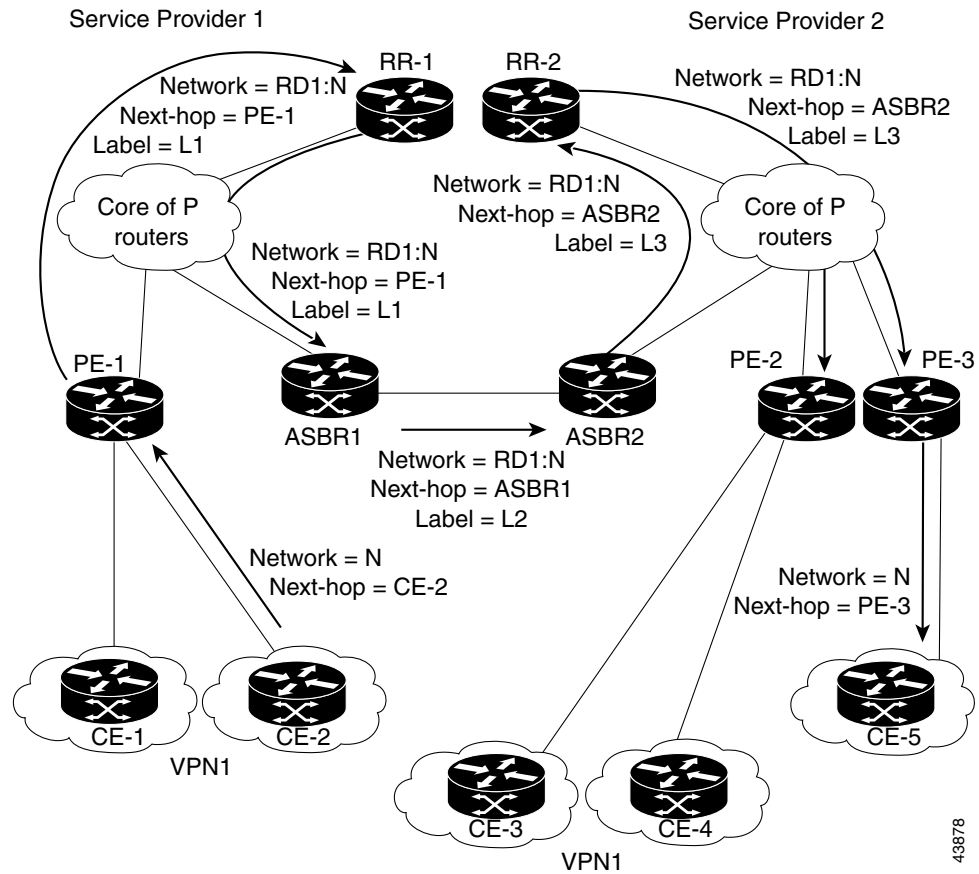
**Figure 13-2** Exchanging Routes and Labels Between Two Autonomous Systems

Figure 13-3 illustrates the exchange of VPN route and label information between autonomous systems. The only difference is that ASBR2 is configured with the **redistribute connected** command, which propagates the host routes to all PEs. The **redistribute connected** command is necessary because ASBR2 is not the configured to change the next hop address.

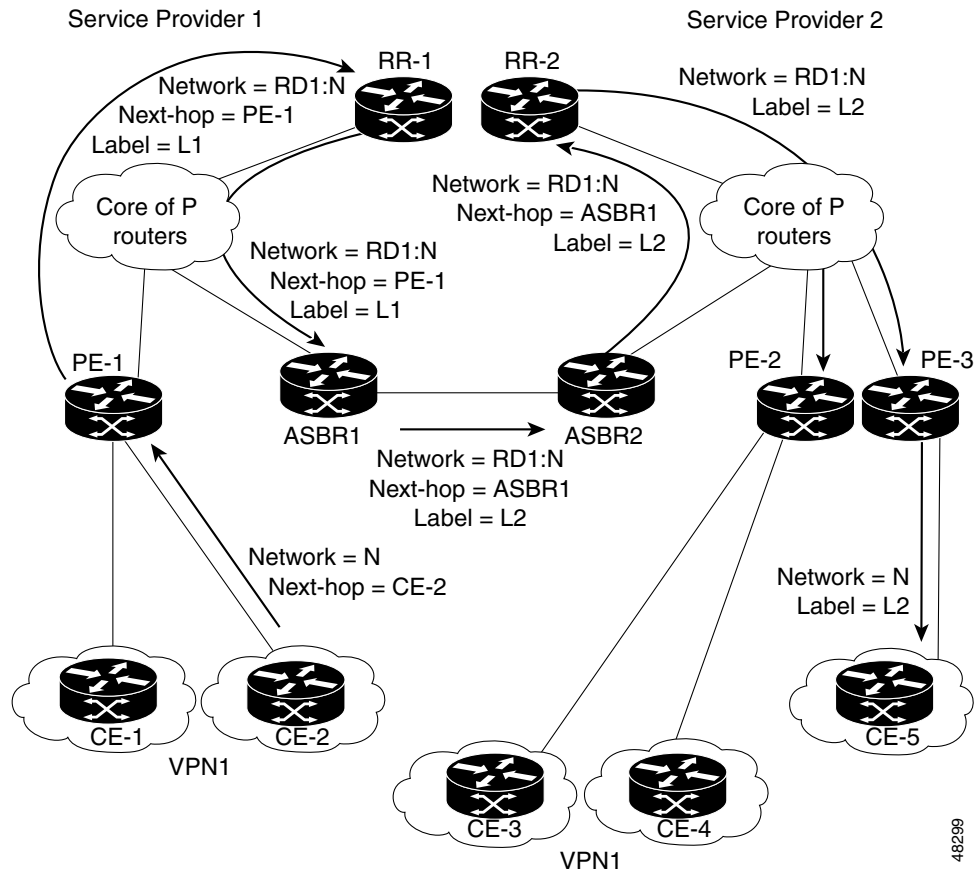
**Figure 13-3** Host Routes Propagated to All PEs Between Two Autonomous Systems

Figure 13-4 illustrates how packets are forwarded between autonomous systems in an interprovider network using the following packet forwarding method:

Packets are forwarded to their destination via MPLS. Packets use the routing information stored in the LFIB of each PE router and EBGp border edge router. The service provider VPN backbone uses dynamic label switching to forward labels.

Each autonomous system uses standard multi-level labeling to forward packets between the edges of the autonomous system routers (for example, from CE-5 to PE-3). Between autonomous systems, only a single level of labeling is used, corresponding to the advertised route.

A data packet carries two levels of labels when traversing the VPN backbone:

- The first label (*IGP route label*) directs the packet to the correct PE router or EBGp border edge router. (For example, the IGP label of ASBR2 points to the ASBR2 border edge router.)
- The second label (*VPN route label*) directs the packet to the appropriate PE router or EBGp border edge router.

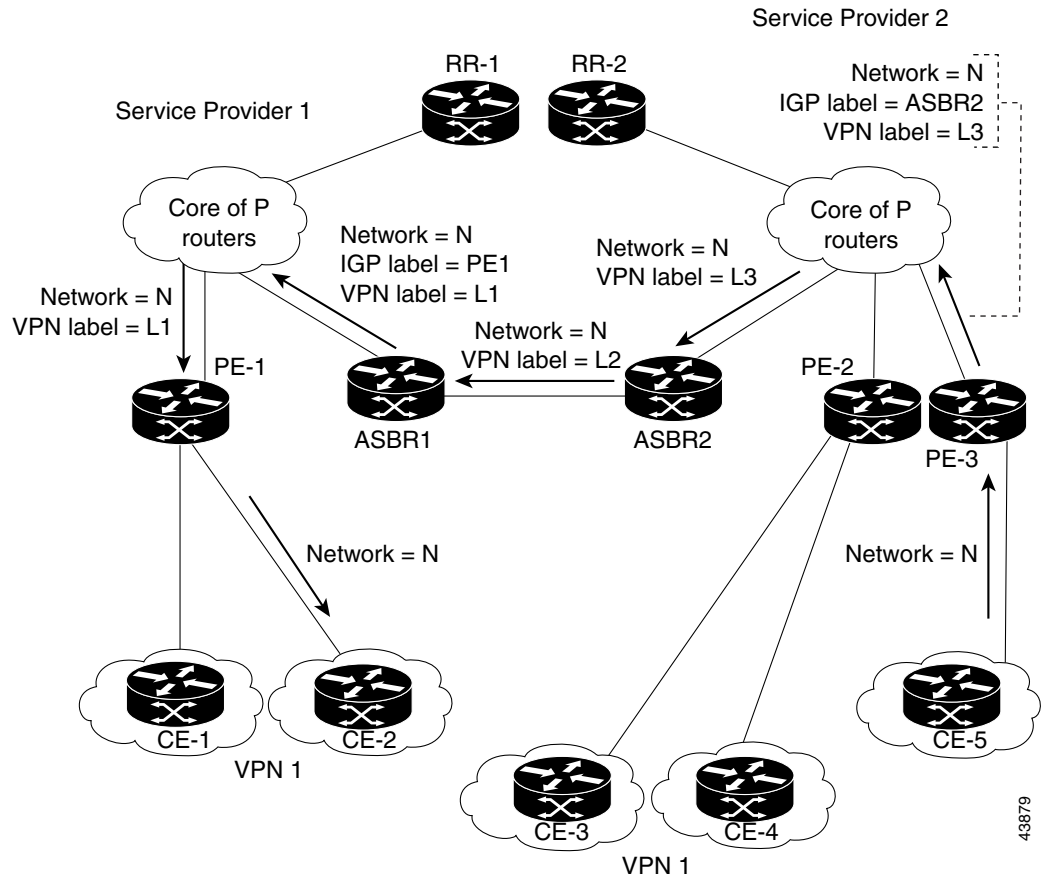
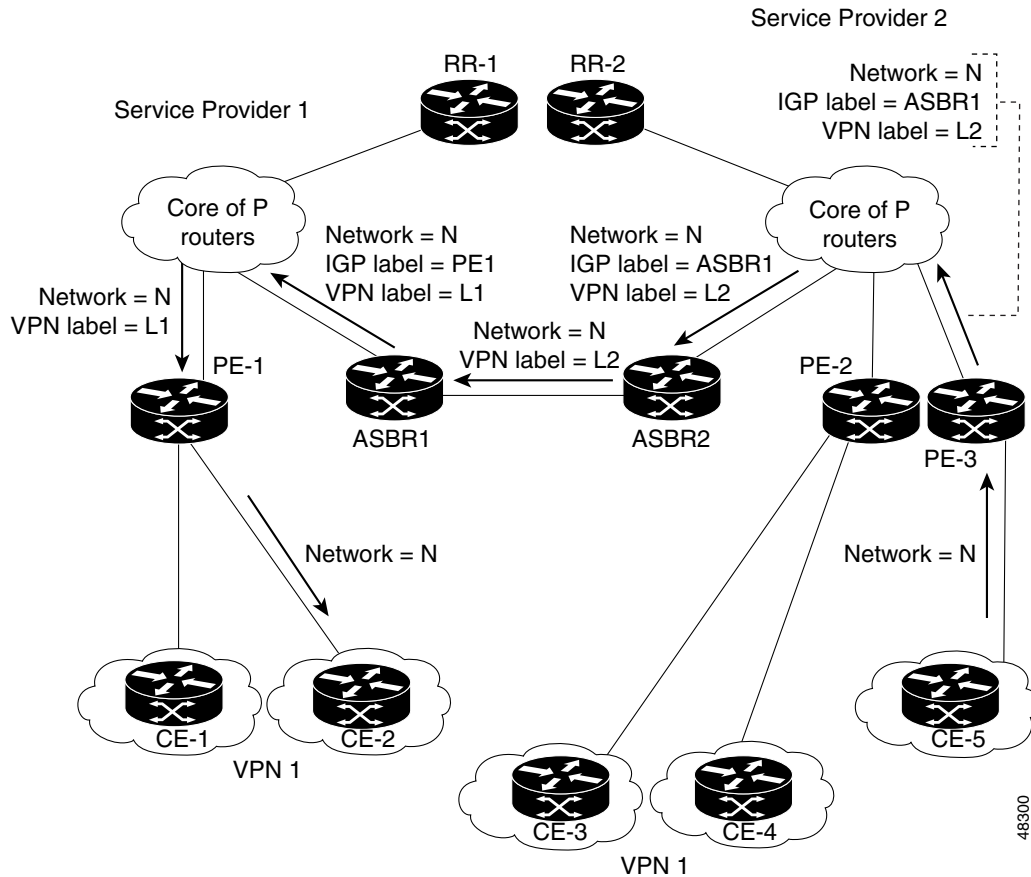
**Figure 13-4 Forwarding Packets Between Two Autonomous Systems**

Figure 13-5 illustrates shows the same packet forwarding method, except the EBGP router (ASBR1) forwards the packet without reassigning it a new label.

**Figure 13-5 Forwarding Packets Without Reassigning a New Label**

## Routing Between Subautonomous Systems in a Confederation

A VPN can span service providers running in separate autonomous systems or between multiple subautonomous systems that have been grouped together to form a confederation.

A confederation reduces the total number of peer devices in an autonomous system. A confederation divides an autonomous system into subautonomous systems and assigns a confederation identifier to the autonomous systems.

In a confederation, each subautonomous system is fully meshed with other subautonomous systems. The subautonomous systems communicate using an IGP, such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS). Each subautonomous system also has an EBGp connection to the other subautonomous systems. The confederation EBGp (CEBGp) border edge routers forward next-hop-self addresses between the specified subautonomous systems. The next-hop-self address forces the BGP to use a specified address as the next hop rather than letting the protocol choose the next hop.

You can configure a confederation with separate subautonomous systems in two ways:

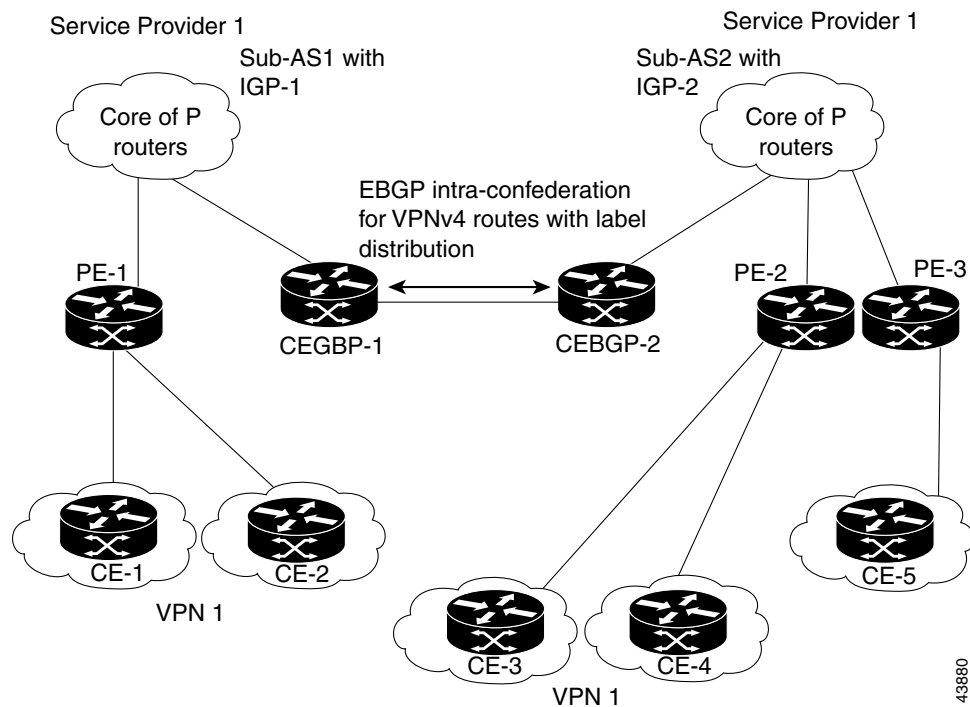
- You can configure a router to forward next-hop-self addresses between only the CEBGP border edge routers (both directions). The subautonomous systems (IBGP peers) at the subautonomous system border do not forward the next-hop-self address. Each subautonomous system runs as a single IGP domain. However, the CEBGP border edge router addresses are known in the IGP domains.

- You can configure a router to forward next-hop-self addresses between the CEBGP border edge routers (both directions) and within the IBGP peers at the subautonomous system border. Each subautonomous system runs as a single IGP domain but also forwards next-hop-self addresses between the PE routers in the domain. The CEBGP border edge router addresses are known in the IGP domains.

Figure 13-6 illustrates a typical MPLS VPN confederation configuration. In this confederation configuration:

- The two CEBGP border edge routers exchange VPN-IPv4 addresses with labels between the two subautonomous systems.
- The distributing router changes the next-hop addresses and labels and uses a next-hop-self address.
- IGP-1 and IGP-2 know the addresses of CEBGP-1 and CEBGP-2.

**Figure 13-6 EGBP Connection Between Two AS's in a Confederation**



In this confederation configuration:

- CEBGP border edge routers function as neighboring peers between the subautonomous systems. The sub-autonomous systems use EGBP to exchange route information.
- Each CEBGP border edge router (CEBGP-1, CEBGP-2) assigns a label for the route before distributing the route to the next subautonomous system. The CEBGP border edge router distributes the route as a VPN-IPv4 address by using the multiprotocol extensions of BGP. The label and the VPN identifier are encoded as part of the NLRI.
- Each PE and CEBGP border edge router assigns its own label to each VPN-IPv4 address prefix before redistributing the routes. The CEBGP border edge routers exchange VPN-IPv4 addresses with the labels.

The next-hop-self address is included in the label (as the value of the EBGP next-hop attribute). Within the sub-autonomous systems, the CEBGP border edge router address is distributed throughout the IBGP neighbors and the two CEBGP border edge routers are known to both confederations.

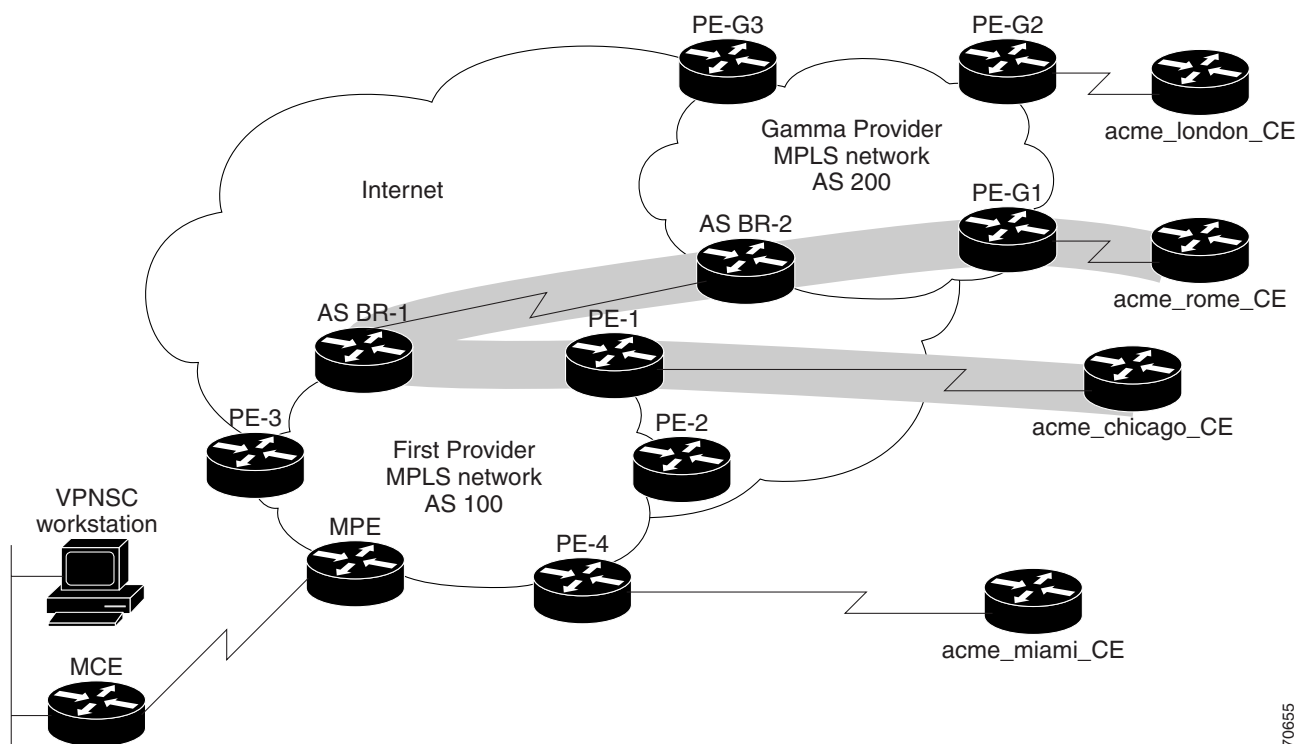
## Using ISC to Span Multiple Autonomous Systems

As described in *Exchanging VPN Routing Information*, page 13-4, autonomous systems exchange VPN routing information (routes and labels) to establish connections. To control connections between autonomous systems, the PE routers and Exterior BGP ASBRs (Autonomous System Boundary Routers) maintain a Label Forwarding Information Base (LFIB). The LFIB manages the labels and routes that the PE routers and EBGP border edge routers receive during the exchange of VPN information.

The ASBRs are configured to change the next hop (next-hop-self) when sending VPN-IPv4 network layer reachability information to their IBGP neighbors. Therefore, the ASBRs must allocate a new label when they forward the NLRI to their IBGP neighbors.

Figure 13-7 shows the example ISC network used in this section.

**Figure 13-7** Example VPN Network with Two Autonomous Systems



In order for traffic from Acme\_Chicago in AS 100 to reach Acme\_Rome in AS 200, ISC must provision two links only:

- The link between Acme\_Chicago and PE-1
- The link between Acme\_Rome and PE-G1

As shown in Figure 13-7, ISC routes the VPN traffic from PE-1 to ASBR-1, from ASBR-1 to ASBR-2, then from ASBR-2 to PE-G1; finally the traffic is routed to its destination, Acme-Rome.

ASBR-1 and ASBR-2 must run BGP (Border Gateway Protocol). Then iMP-BGP (interior Multiprotocol BGP) handles the routes between PE-1 to ASBR-1 in AS 100 and the routes between PE-2 to ASBR-2 in AS 200. eMP-BGP (exterior Multiprotocol BGP) handles the routes between ASBR-1 and ASBR-2.

**Tip**

---

The service provider must configure a VPN-IPv4 EBGP session between directly connected Autonomous System Boundary Routers (ASBRs). This is a one-time setup procedure that the service provider must manage. ISC does not provision the link between the ASBR devices that span autonomous systems.

---

A VPN-IPv4 address (also referred to as a *VPNv4* address) is the combination of the IPv4 address and the 8-byte route distinguisher (RD). Combining the RD and the IPv4 address makes the IPv4 route globally unique across the MPLS VPN network. BGP considers an IPv4 address as different from another IPv4 address that has the same network and subnet mask when the route distinguishers are different.





## Generating MPLS Reports

---

This chapter provides information on generating MPLS reports. It contains the following sections:

- Overview, page 14-1
- Accessing MPLS Reports, page 14-1
- MPLS PE Service Report, page 14-3
- Running Reports, page 14-4
- MPLS Service Request Report, page 14-5
- Creating Custom Reports, page 14-6

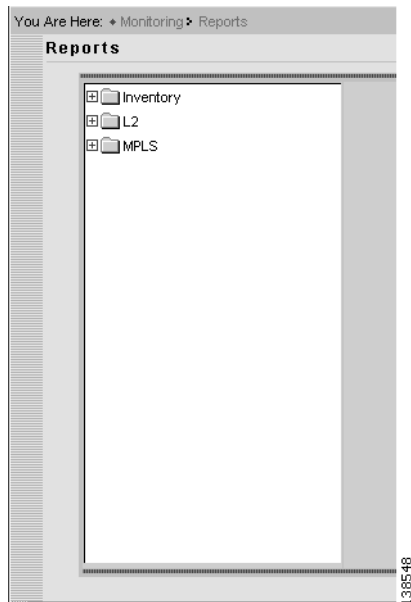
### Overview

The ISC reporting GUI is used across multiple ISC modules, including MPLS. For a general coverage of using the reports GUI, running reports, using the output from reports, and creating customized reports, see “Monitoring” chapter in *Cisco IP Solution Center Infrastructure Reference, 4.1*. The rest of this chapter provides information about the MPLS reports available in ISC.

### Accessing MPLS Reports

---

- Step 1** To access the reports framework in the ISC GUI, choose **Monitoring > Reports**.
- Step 2** Click on the MPLS folder to display the available MPLS reports.  
The Reports window appears, see Figure 14-1.

**Figure 14-1** Reports Window

- Step 3** From the reports listed under MPLS in the left navigation tree, click on the desired report to bring up the window associated with that report.
- 

**Note**

Several sample reports are provided in the MPLS 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, along with the supported reports, as a basis for creating your own custom reports. See “Creating Custom Reports” section on page 14-6 for information on custom reports.

---

# MPLS PE Service Report

The MPLS Service report allows you to choose PEs and display their roles (for example, N-PE, U-PE or PE-AGG) and MPLS-related services that are running on them.

Click the MPLS Service Report icon to bring up the window for this report, as shown in Figure 14-2.

**Figure 14-2 MPLS PE Service Report**

Layout	
Title:	MPLS PE Service Report
Chart Type:	Tabular
Filters (All field values are required, * or a valid value.)	
PE Role:	*
PE Name:	*
Sorting	
Field:	PE Role Ascending
Output Fields	
PE Role PE Name Policy Type SR State SR ID SR Job ID	

## Filter Values

- **PE Role** – PE device role (N-PE, U-PE, or PE-AGG).
- **PE Name** – PE device name.

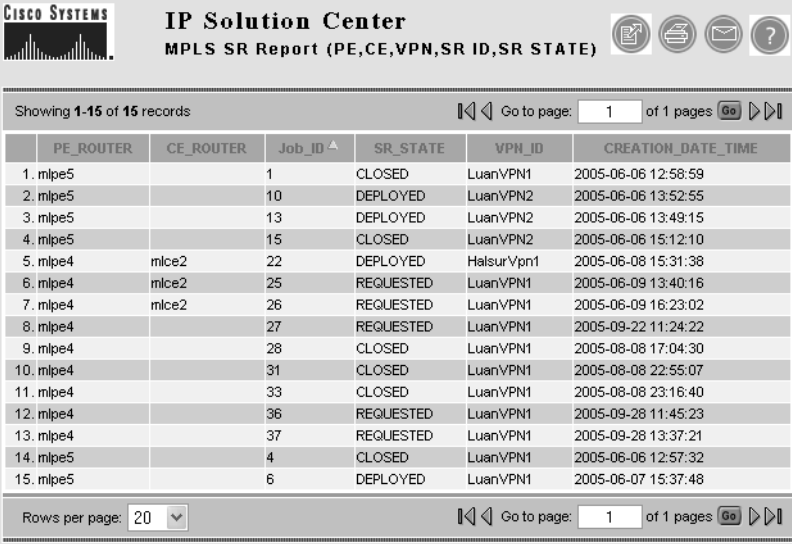
## Output Values

- **PE Role** – List by PE device role (N-PE, U-PE, or PE-AGG).
- **PE Name** – List by PE device name.
- **Policy Type** – List by type of Policy.
- **SR State** – List by service request state (see Appendix B, “Service Request Transition States”).
- **SR ID** – list by service request ID.
- **SR Job ID** – List by service request job ID.

# Running Reports

To run the report, click **View** in the lower right corner of the report window. This generates the report output. An example of an MPLS service request report output is shown in Figure 14-3.

**Figure 14-3** Report Output



**CISCO SYSTEMS** **IP Solution Center**  
MPLS SR Report (PE,CE,VPN,SR ID,SR STATE)

Showing 1-15 of 15 records Go to page: 1 of 1 pages

	PE_ROUTER	CE_ROUTER	Job_ID ▲	SR_STATE	VPN_ID	CREATION_DATE_TIME
1.	mlpe5		1	CLOSED	LuanVPN1	2005-06-06 12:58:59
2.	mlpe5		10	DEPLOYED	LuanVPN2	2005-06-06 13:52:55
3.	mlpe5		13	DEPLOYED	LuanVPN2	2005-06-06 13:49:15
4.	mlpe5		15	CLOSED	LuanVPN2	2005-06-06 15:12:10
5.	mlpe4	mlce2	22	DEPLOYED	HalsurVpn1	2005-06-08 15:31:38
6.	mlpe4	mlce2	25	REQUESTED	LuanVPN1	2005-06-09 13:40:16
7.	mlpe4	mlce2	26	REQUESTED	LuanVPN1	2005-06-09 16:23:02
8.	mlpe4		27	REQUESTED	LuanVPN1	2005-09-22 11:24:22
9.	mlpe4		28	CLOSED	LuanVPN1	2005-08-08 17:04:30
10.	mlpe4		31	CLOSED	LuanVPN1	2005-08-08 22:55:07
11.	mlpe4		33	CLOSED	LuanVPN1	2005-08-08 23:16:40
12.	mlpe4		36	REQUESTED	LuanVPN1	2005-09-28 11:45:23
13.	mlpe4		37	REQUESTED	LuanVPN1	2005-09-28 13:37:21
14.	mlpe5		4	CLOSED	LuanVPN1	2005-06-06 12:57:32
15.	mlpe5		6	DEPLOYED	LuanVPN1	2005-06-07 15:37:48

Rows per page: 20 Go to page: 1 of 1 pages

In the current release of ISC, the reports GUI supports output in tabular format. The output is listed in columns, which are derived from the outputs you selected in the reports window.

Each row (or record) represents one match of the search criteria you set using the filter fields in the reports window.

The column heading with a triangle icon is the output that the records are sorted by. By clicking on any column heading, you can toggle between ascending and descending sort order. To sort on another output value, click on the heading for that value.

# MPLS Service Request Report

The MPLS Service Request report feature allows you to list service requests as related to PE, CE, VPN, SR ID, SR STATE.

Click the MPLS Service Request Report icon to bring up the window for this report, as shown in Figure 14-4.

**Figure 14-4 MPLS Service Request Report**

Layout	
Title:	MPLS SR Report (PE,CE,VPN,SR ID,SR STATE)
Chart Type:	Tabular
<b>Filters (All field values are required, * or a valid value.)</b>	
PE_ROUTER:	* <input type="text"/> <input type="button" value="Select"/>
CE_ROUTER:	* <input type="text"/> <input type="button" value="Select"/>
Job_ID:	* <input type="text"/>
SR_STATE:	* <input type="text"/>
VPN_ID:	* <input type="text"/> <input type="button" value="Select"/>
<b>Output Fields</b>	
PE_ROUTER CE_ROUTER Job_ID SR_STATE VPN_ID CREATION_DATE_TIME	
<b>Sorting</b> N/A	

## Filter Values

- **PE ROUTER** – Choose some or all (\*) PE routers.
- **CE ROUTER** – Choose some or all (\*) CE routers.
- **Job ID** – Service request job IDs.
- **SR STATE** – Service Request states (see Appendix B, “Service Request Transition States”).
- **VPN ID** – Choose some or all (\*) VPNs by ID.

## Output Filters

- **PE ROUTER** – Show PE routers.
- **CE ROUTER** – Show CE routers.
- **Job ID** – List by Job ID.
- **VPN ID** – List by VPN ID.
- **CREATION DATE TIME** – List by date and time report created.

# Creating Custom Reports

The reports listed in the ISC GUI in the MPLS 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/mpls\_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.



## IP Solution Center—MPLS VPN

---

This chapter describes an overview of the Cisco IP Solution Center (ISC) Multiprotocol Label Switching (MPLS) virtual private network (VPN) system solution. This chapter contains the following major sections:

- IP Solution Center Overview, page A-1
- Service Provider Network, page A-12
- MPLS VPN Security, page A-27

### IP Solution Center Overview

This section contains the following sections:

- Business Application, page A-1
- System Architecture, page A-2
- System Features, page A-7

### Business Application

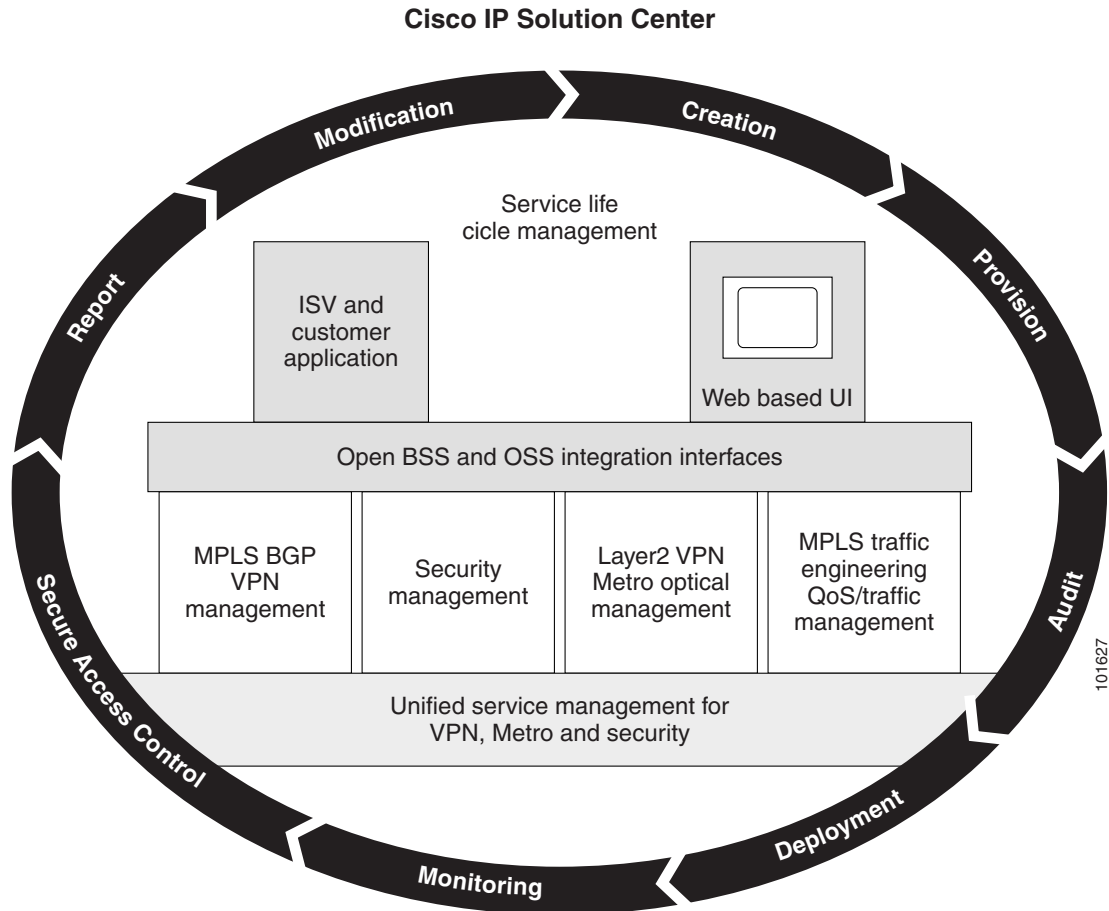
ISC is a carrier-class network and service-management solution, designed especially for Cisco routing, switching, and security products. ISC addresses a growing customer demand for provisioning IP-based services with a single management platform.

ISC provides IP-based services in four primary applications:

- MPLS VPN management
- Layer 2 VPN management
- Managed Security for IP security (IPsec) VPN, firewall, and Network Address Translation (NAT) management - **IPsec, NAT, and Firewall are not supported in this release. -**
- Policy-based quality of service (QoS)

ISC provides a robust and centralized management platform that can manage the entire life-cycle of IP-based services, integrate with existing network management infrastructures, and easily accommodate the implementation of emerging new technologies.

Figure A-1 shows how ISC integrates into the network life-cycle management process.

**Figure A-1** *ISC Network Life-Cycle Management Process*

ISC is also a scalable solution for service deployment. Service providers need a deployment tool if they want to deploy more than a relatively small number of VPNs. And a tool that can allocate and track the various number pools (IP addresses, RT, RD, VLAN ID, and VC ID) simplifies the service deployment model.

ISC integrates with other Cisco network management tools. Though not seen as a network monitoring tool in itself, ISC has an audit capability that allows service provider to track the validity of provisioned VPNs and other services. Through the SLA deployment capability, SNMP data can be generated on a per-VPN basis.

## System Architecture

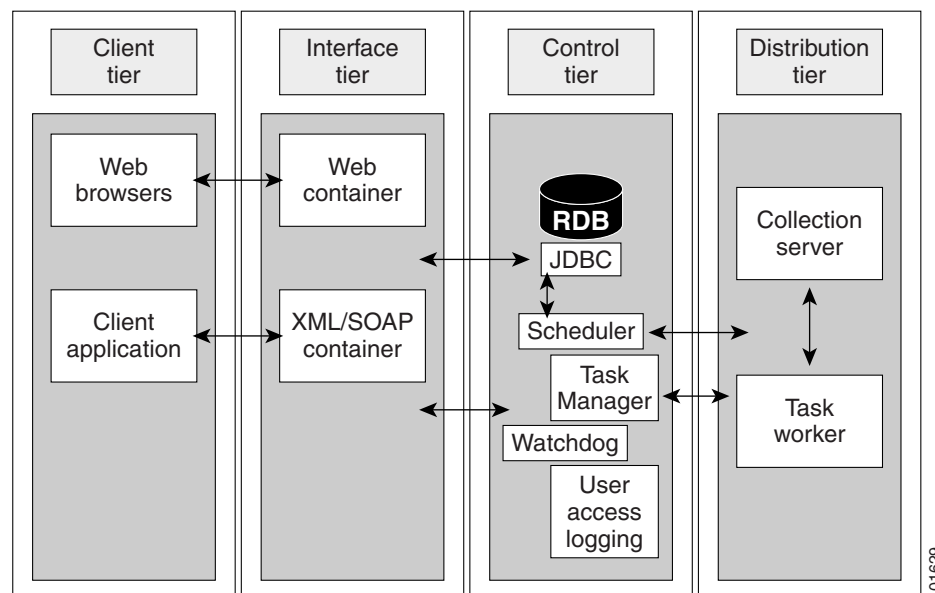
ISC features a four-tier, modular architecture with a distributed design and an emphasis on high performance, scalability, and availability.

The four tiers consist of the following components:

- Client Tier: Web Browser or Client Application
- Interface Tier: Web Servers or Server Farms
- Control Tier: Master Server and Database
- Distribution Tier: Processing and Collection Servers

Figure A-2 shows the four-tiered architecture.

**Figure A-2 Four-Tiered ISC Architecture**



### Client Tier

The client tier consists of web browsers (GUI) and client applications that access ISC through the application programming interface (API). Customers do not have to access ISC through the GUI. The northbound API can perform all system functions. The API allows you to tightly integrate ISC with your OSS environment. The web browsers communicate with the ISC web server through HTTP. The client applications communicate with the ISC CORBA server (the backward compatible API) or Web Server by way of XML/SOAP (the new API).

### Interface Tier

The interface tier contains one or more web servers in a web farm. As more operators need to access the system, the web farm can be scaled up by adding new web servers to the farm. The interface tier provides horizontal scalability for handling a large number of users. It also provides high availability. When one server in the farm goes away, the whole system continues to function and users can continue to interact with the system through other interface tier machines. This system allows the dynamic addition and removal of machines to and from the web farm.

### Control Tier

The control tier consists of the ISC Repository (a relational database) and the task scheduling and distribution system. In ISC, there is only one control tier server. It is called the Master server. The Master server is the “nerve center” of the infrastructure; you can consider it identical to the ISC workstation itself. All vital information is stored in the Repository on the Master server. The Master server controls how tasks are distributed to the back-end system.

### Distribution Tier

The distribution tier consists of the Processing servers and Collection servers. Each Processing server or Collection server runs on its own physical machine. Processing servers are responsible for executing tasks such as provisioning, auditing, SLA data collection, and so on. There can be one or more Processing server machines.

A collection server is responsible for interacting with the network devices. For example, configuration upload and download to a Cisco router is through its Collection server. In other words, each Collection server owns a set of network devices. Collection servers and their geographically related network devices are organized into *collection zones*. There can be one or more Collection servers per installation. A Collection server is called into service when data is needed from one of the devices that it owns.

**Note**

Although the Web server, the Master server, the Processing server, and the Collection server are normally installed on different physical machines for large installations, they can be collapsed into a single machine for a small installation. In this case then, there is only one instance of the Web server, Processing server, and Collection server.

### Additional Features

The ISC design has the following additional features:

- Addresses scalability at the front-end (client and interface tiers) and back-end (control and distribution tiers).
- Ensures consistency of data and visibility among applications, with a cohesive service model.
- Interface Tier: Sustains many concurrent users. Can be separate hardware, web-based multi-access.
- Control Tier: Central control and system monitoring.
- Distribution Tier: Supports large numbers of concurrent running tasks. Can be separate hardware.

The ISC four-tier architecture allows scaling at any level on any or all of the four tiers.

For instance, if deployment operators are in widely scattered locations, multiple interface servers can be deployed to speed the input of these operators. Also, given that the slowest part of the deployment process is connecting to the network devices involved, multiple provisioning servers can be controlled by a single Master server. Complete management of all servers can be conducted from a single point, the Master server.

The built-in Watchdog process on all servers restarts server processes as necessary, and all distributed Watchdog servers report to the Master server Watchdog process.

The Distribution Tier can be scaled horizontally to support a large number of concurrent running tasks. The software architecture consists of two major subsystems, the Processing Server and the Collection Server. Jobs are distributed to the Processing Servers in parallel by the Task Manager and Job Distribution Framework.

Each Processing and Collection Server has a watchdog process that reports statistics and health information to the Master Watchdog. All remote servers are monitored and configured from the Central Location (Master in Control Tier).

The Master server verifies the presence of the collection and processing servers by sending a keep-alive (heartbeat polling).

## Load Balancing

The major aspects of distributed load balancing in ISC are as follows:

- The Master server (which can be considered to be identical to the ISC Solaris workstation) distributes jobs to processing servers by way of a sophisticated load-balancing algorithm.
- The Processing server can be added dynamically. The Watchdog will discover their existence when you start up ISC.
- Each Collection server is responsible for a set of *collection zones*. Each zone has one Collection Server.
- Both Processing servers and Collection servers failover to the Master server automatically.
- Each device belongs to a *zone*, but a device can be relocated to a different zone as needed.

If the service provider has implemented one or more Processing servers or Collection servers, all the servers—Master, Processing, and Collection servers—are listed in the Administration Control Center.

The Remote server can also be installed from the Control Center.

All Remote servers are monitored by Watchdogs. Remote Watchdogs report statistics to the Master Watchdog. You can start and stop all the servers from the Administration Control Center. Logs are available for viewing in real time.

Figure A-3 shows the topology for a simple flat-based load-balancing configuration.

**Figure A-3 Simple Flat-Based Server Load Balancing Configuration**

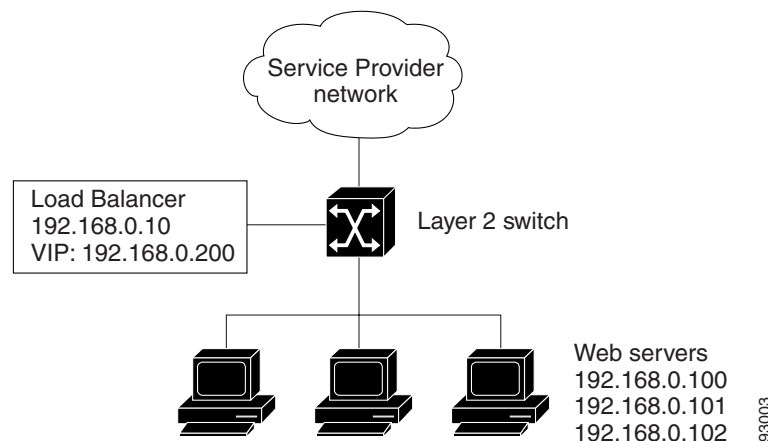
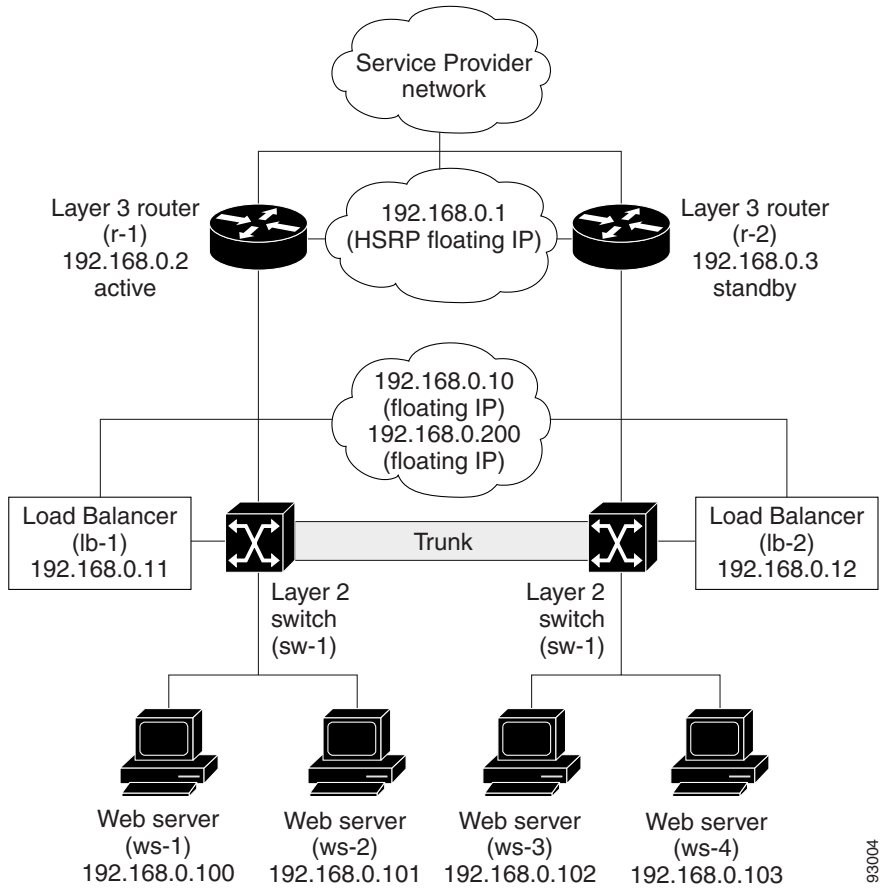


Figure A-4 on page A-6 shows a flat-based route-path server load balancing configuration with redundancy built into the topology.

Figure A-4 Redundant Load Balancing Configuration



93004

## System Features

Table A-1 describes the ISC system features.

**Table A-1**      **ISC System Features**

Feature	Description	Benefit
Auto-Discovery of MPLS VPN Services	Discovers MPLS VPN services that were configured prior to ISC activation on the service provider network	Service providers could have manually configured several MPLS VPN services for customers. To continue managing these services, ISC MPLS VPN Service Discovery can be used to discover these services and continue managing them using ISC.
Automatic Resource Allocation	<ul style="list-style-type: none"> <li>Allows the automatic allocation of parameters during MPLS VPN provisioning such as Router Target (RT), Route Distinguisher (RD), AS (Autonomous System Number for BGP Version 4), and VRF name</li> <li>Enables the service operator to automatically allocate resources such as IP addresses, VLAN, Route Distinguisher, and Router Target</li> </ul>	Automatic Resource Assignment relieves the service operator from manually entering certain parameters during service activation. ISC keeps track of all the allocated resources and to which service, customer, or site these resources were allocated.
Backup and Restore	ISC has the system capability to make backups of your database and to restore data from a backup.	The backup and restore capabilities of ISC protect your data against operating system crashes, file corruption, disk failures, and total machine failure.
Distributed architecture	ISC is a four-tiered system consisting of client, interface, control, and distribution tiers.	Offers a scalable and reliable architecture for large-scale operations.
Grey Management VPN	Supports the management MPLS VPN. All the CEs that are managed by service providers can also be added to the management VPN	All service provider managed CEs can be added to the grey management VPN in order to be managed and monitored
Inter-AS Management	Manages the provisioning of inter-AS MPLS VPN Services.	The provisioning across AS can be problematic. In MPLS VPN, multiple providers can inter-operate their network using different BGP Autonomous System numbers
L2 Access into MPLS VPN	ISC allocates VLANs for customers and maps the VLAN to a MPLS VPN at the PE level	<p>Using Ethernet switches to distribute service to customers is one of the most cost-effective ways to deliver services. ISC can handle L2 Access Domain with aggregation or ring topologies.</p> <p>In more and more cases, service providers utilize L2 Ethernet switches to distribute their services to customers. L2 Access Domain can be in an aggregation or ring topology.</p>

**Table A-1** *ISC System Features (continued)*

Feature	Description	Benefit (continued)
Managed and Unmanaged CE	Handles managed and unmanaged CPE	ISC smart management can handle the managed and unmanaged CE scenarios.
MPLS VPN Carrier Supporting Carrier (CSC) Support	MPLS supports the Carrier supporting Carrier (CSC) deployment scenario using LDP/IGP and BGP/MPLS.	The carrier supporting carrier feature enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network.
Multicast VPN	Allows service providers to support multicast traffic in a MPLS VPN environment	ISC offers the configuration and monitoring of Multicast MPLS VPNs.  MPLS VPNs only support unicast traffic connectivity. Deploying the Multicast VPN feature in conjunction with MPLS VPN allows service providers to offer both unicast and multicast connectivity to MPLS VPN customers.
Northbound Interface CORBA and XML over HTTP	Integrates with other OSS FCAPS applications; ISC provides CORBA for backward compatibility with VPNSC 2.2 and, going forward, provides XML over HTTP/HTTPS	Other FCAPS OSS applications need access to ISC VPN topology information, by way of its northbound interface, to offer flow-through provisioning, extracting the VPN customer information, for example, for any fault application.
Policy-Based Provisioning	Defines provisioning parameters in a Service Policy to be used during service activation	A Service Policy captures provisioning parameters, such as PE-CE protocol, IP numbering, and VLAN Auto-Allocation.  Using Service Policies for service activation greatly reduces the workload for service operators. Parameters required for service activation are captured up front in the service policy.
Provisioning Based on Current Network	Uploads the configuration of the network elements to calculate the delta configuration needed to have a successful service activation, prior to service activation	There is always a possibility that the network configuration could have varied since the last snap-shot. By uploading the configuration prior to applying the configuration, ISC ensures that the service activation configuration will be successfully applied and will not collide with the existing configuration.
Quality of Service (QoS) Provisioning	A QoS service policy captures all the QoS provisioning parameters for a collection of access circuits between a CE and PE.	QoS service policy greatly reduces the service operator's tasks because it allows the configuration of QoS parameters and their association to access circuits.
Role-based Access Control	Implements Role-based Access Control that gives very granular access privileges to ISC users	Role-based Access Control gives access control to the service providers who want to implement strict operational processes.

**Table A-1**      **ISC System Features (continued)**

Feature	Description	Benefit (continued)
Routing Protocols	<ul style="list-style-type: none"> <li>• OSPF</li> <li>• EIGRP</li> <li>• RIP</li> <li>• Static</li> <li>• BGP</li> </ul>	ISC offers most widely used routing protocols for PE-CE links.
Thin Client Web GUI	Provides a web-based thin client for user interface	ISC offers a thin web-based client that is easy to use. Network operators require less training.
VRF Lite and Multi-VRF CE	VRF Lite CE management	ISC offers VRF Lite CE for enhanced VPN traffic separation and security up to the CE.

## Template Manager

The Template Manager in ISC is a provisioning system that provides fast, flexible, and extensible Cisco IOS command generation capability. The Template Manager defines standard templates to generate Cisco IOS configurations for common provisioning tasks, such as common IPv4, QoS, and VPN provisioning.

- A *template file* is a file created by the Template Manager that stores a ISC template definition.
- A *template data file* is a text file that stores variable values to generate the template file. A valid data file contains name-value pairs for all the variables defined in a template. Each template file can be associated with multiple data files; however, note that each data file can only be associated with a single template. You can select which data file to use to generate a template. The filename suffix for data files is *.dat*.
- A *template configuration file* is an IOS configuration file that stores the Cisco IOS commands created by the Template Manager. A template configuration file can be either a partial or complete configuration file. When you generate a template configuration file using a particular data file, the template configuration filename is the same as the data file's name.

The template data files are tightly linked with its corresponding template. You can use a data file and its associated template to create a template configuration file. The template configuration file is merged with (either appended to or prepended to) the ISC configlet. ISC downloads the combined configlet to the edge device router.

You can apply the same template to multiple edge devices, assigning the appropriate template data file for each device. Each template data file includes the specific data for a particular device (for example, the management IP address or host name of each device).

The template files and data files are in XML format. The template file, its data files, and all template configuration file files are mapped to a single directory.

- ISC creates the initial ISC configlet. Through the Template Manager, you can create a template configuration file. You can then associate a template configuration file with a service request, which effectively merges the ISC configlet and the template configuration file. You can then download this merged ISC configlet to the target router (or routers).
- You can also create a template configuration file and download it directly to a router.

Service providers can use the Template Manager to enhance ISC functionality. You can use the Template Manager to provide initial configuration for any service provider core device or edge device.

The Template Manager can be used as a stand-alone tool to generate complete configuration files that you can download to any ISC target.

Some of the additional uses for templates are as follows:

- IOS firewall provisioning - **Firewall is not supported in this release.** -
- Add a set of commands that ISC does not include to a service request; for example, provisioning ATM Class of Service.
- Use the template feature to apply Class of Service using IP connectivity.

Download a ISC service request and an Cisco IOS configuration file in one download operation through the console. This edge device staging method would create a template and apply the service request in one step.

## Role-Based Access Control (RBAC)

The central notion of role-based access control (RBAC) is that permissions are associated with *roles*, and users are made *members* of appropriate roles. Access control policy is embodied in various components of RBAC, such as role-permission, user-role, and role-role relationships. These components determine whether a particular user will be allowed to access a particular piece of data in the system.

The Role object specifies a set of occupants and the privileges or permissions granted to those occupants. There are several ways for constructing a role.

A role can represent competency to do specific tasks, such as a technician or a support engineer. A technician can collect edge device and interface information and import them into the ISC Repository. A support engineer (service operator) can create policies, submit service requests and deploy them.

A role can reflect specific duty assignments, for example, an engineer can be assigned to provision customer Acme's VPN. The operator might not be allowed to provision the competitor customer Widget's VPN.

A role can have distinct authority, for example, VPN customer AcmeInc should be allowed only to view or make minor change on Acme's VPN data. The customer should not be allowed to access any other customer's VPN data.

There can be a role hierarchy in which a *super user* has all the permissions allowed to two different roles.

The service provider can define a role for each VPN customer, for example Acme and Widgets. The acme\_customers role and the Widgets\_customers role are mutually exclusive roles. The same user can be assigned to no more than one role in a mutually exclusive set. *Role constraint* supports separation of duties.

ISC supports full Role-Based Access Control to the system resources. Each Role defines limited access to the resources with a set of permissions: view, create, update, delete, and execute. This same access mechanism is also given to a group. When a user is part of a group, he inherits the group's access privileges.

Each user can be assigned one or many roles. Each user will be shown only the resources and services that he or she is allowed to create view, modify, or delete. Using the access privileges that the user has been allocated, the display and action allowed are adjusted accordingly.

## North Bound Interface (NBI)

The user's Web browsers communicate with IP Solution Center Web server through HTTP, and the client applications communicate with ISC's CORBA server (backward compatible API) or through the Web server by way of XML/SOAP.

## API Functionality Supported

API support is provided for the following services:

- QoS Service
- Layer 2 VPN Service
- MPLS VPN Service
- Inventory
- IPsec VPN Service - **IPsec is not supported in this release. -**
- FireWall Service - **Firewall is not supported in this release. -**
- NAT Service - **NAT is not supported in this release. -**
- SLA
- Tasks
- Template Manager

## NBI Benefits

The benefits of the north-bound interface are as follows:

- Supports ISC services and inventory
- XML-based management interface
- Web-based
- Human-readable encoding
- Initial transport support is HTTP/SOAP
- API based on domain manager convergence API

## API Approach

The API approach is as follows:

- Standards based encoding of management operations and payload.
- Layered approach combines need for rigor with flexibility (HTTP, SOAP, CIM Operations, Data Model).
- Leverages XML technology and adds a management framework.
- Allows for polling-based management, event-based management, and synchronous, and asynchronous services.
- Facilities for reliability: event numbering, tagging of requests.
- Facilities for security/RBAC.
- Standardized error semantics.

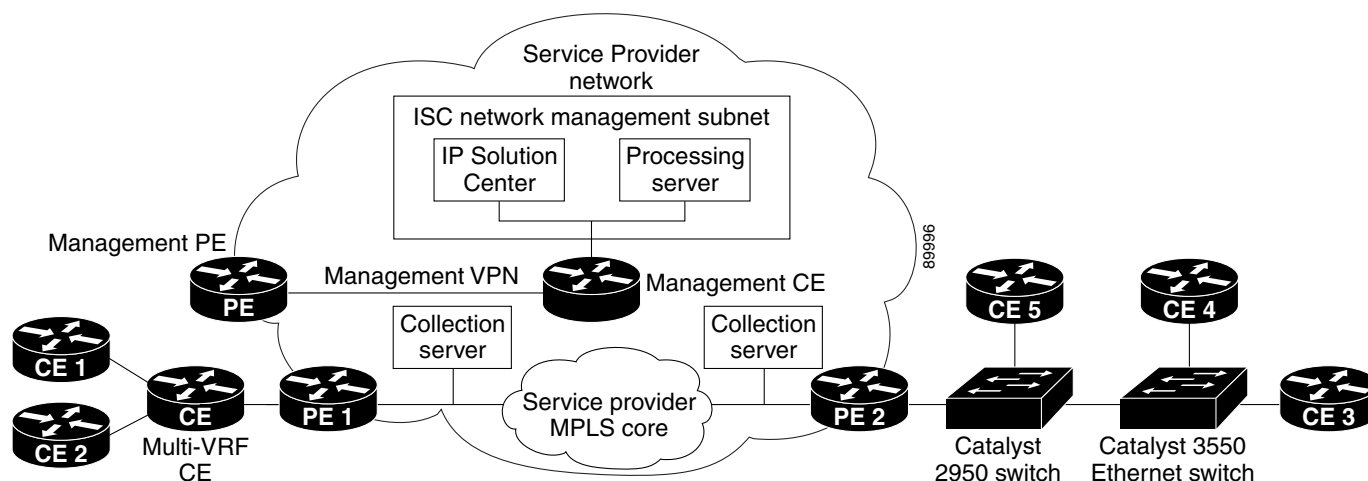
Transport protocol agnostic.

# Service Provider Network

The ISC provisioning engine accesses the configuration files on both the CE and PE to compute the necessary changes to those files that are required to support the service on the PE-CE link. A customer edge router (CE) is connected to a provider edge router (PE) in such a way that the customer's traffic is encapsulated and transparently sent to other CEs, thus creating a virtual private network. CEs advertise routes to the VPN for all the devices in their site.

Figure A-5 shows all the major elements and devices that a service provider can employ to fully deploy ISC MPLS VPN management services.

**Figure A-5** *ISC MPLS VPN Management in the Service Provider Network*



The notable ISC network elements are as follows:

- *ISC Network Management Subnet*

The *ISC Network Management Subnet* is required when the service provider's service offering entails the management of CEs. The management subnet consists of the ISC workstation (where ISC is installed). On the same LAN, the service provider can optionally install one or more Processing servers. The Processing servers are responsible for executing tasks such as provisioning, auditing, SLA data collection, and so on.

- *The Management VPN*

The Management VPN is a special VPN employed by the ISC Network Management Subnet to manage the CEs in a service provider network. Once a CE is in a VPN, it is no longer accessible by means of conventional IPv4 routing, unless the CEs are part of the Management VPN. To communicate with the PEs, the link between the Management PE (MPE) and the Management-CE (MCE) uses a parallel IPv4 link. The Management VPN connects to the managed CEs.

- *Multi-VRF CE*

The Multi-VRF CE is a feature that provides for Layer 3 aggregation. Multiple CEs can connect to a single Multi-VRF CE (typically in an enterprise network); then the Multi-VRF CE connects directly to a PE. Figure A-5 shows CE 1 and CE2 connected to the Multi-VRF CE, and the Multi-VRF CE is connected directly to the PE. For details, see Multi-VRF CE, page A-18.

- *Layer 2 Access to MPLS VPNs*

The service provider can install multiple Layer 2 switches between a PE and CE, as shown in Figure A-5. This feature provides Layer 2 aggregation. Additional CEs can be connected to the switches as well. Cisco supports two switches for the Layer 2 access to MPLS: either a *Cisco Catalyst 2950 Switch* or a *Cisco Catalyst 3550 Intelligent Ethernet Switch*.

- *Collection Servers*

Cisco ISC is designed to provision a large number of devices through its distributed architecture. If the Master server (equivalent to the ISC workstation) cannot keep up with the number of devices, Collection servers can be added to offload the work of the Master server. Among other tasks, Collection servers are responsible for uploading and downloading configuration files to and from Cisco routers.

An MPLS VPN consists of a set of sites that are interconnected by means of an MPLS provider core network. At each site, there are one or more CEs, which attach to one or more PEs. PEs use the Border Gateway Protocol-Multiprotocol (MP-BGP) to dynamically communicate with each other.

It is not required that the set of IPv4 addresses used in any two VPNs be mutually exclusive because the PEs translate IPv4 addresses into IPv4 VPN entities by using MP-BGP with extended community attributes.

The set of IP addresses used in a VPN, however, must be exclusive of the set of addresses used in the provider network. Every CE must be able to address the PEs to which it is directly attached. Thus, the IP addresses of the PEs must not be duplicated in any VPN.

One of ISC key features is to hide much of the complexity in dealing with the deployment of Metro services.

- **Autodiscovery:** ISC supports Autodiscovery of network elements, of network topology, and MPLS VPN services. This feature greatly reduces the initial effort needed to insert ISC in the service provider's operation. For details, see Chapter 2, "Provisioning Unmanaged Multi-VRF CE."
- **Managed CLE:** ISC offers the capability of managing the Customer Located Equipment (CLE), which gives the service provider the possibility of offering a managed Metro Service to their customer (configuration, monitoring, and auditing of the managed CLE).
- **Plug and Play:** As the network and customer base grow, network elements can be added to the network. ISC, working in collaboration with CNS Intelligent Agents, is able to detect newly added Network Elements.

This gives the service provider the ability to rapidly deploy services and network elements.

- **End-To-End Service Management:** ISC manages the entire end-to-end provisioning of MPLS VPN services. Assuming that the network operator defined MPLS VPN service policy and the parameters that are to be editable by the service operator during the provisioning process, ISC translates these service requirements into IOS configurations. ISC does a just-in-time Cisco IOS configuration download, which consist of always validating the configuration of the real devices before applying the needed configuration.

After a service is configured, ISC makes sure that the service configuration is the intended one by checking the configuration and verifying that VPN routing is operational.

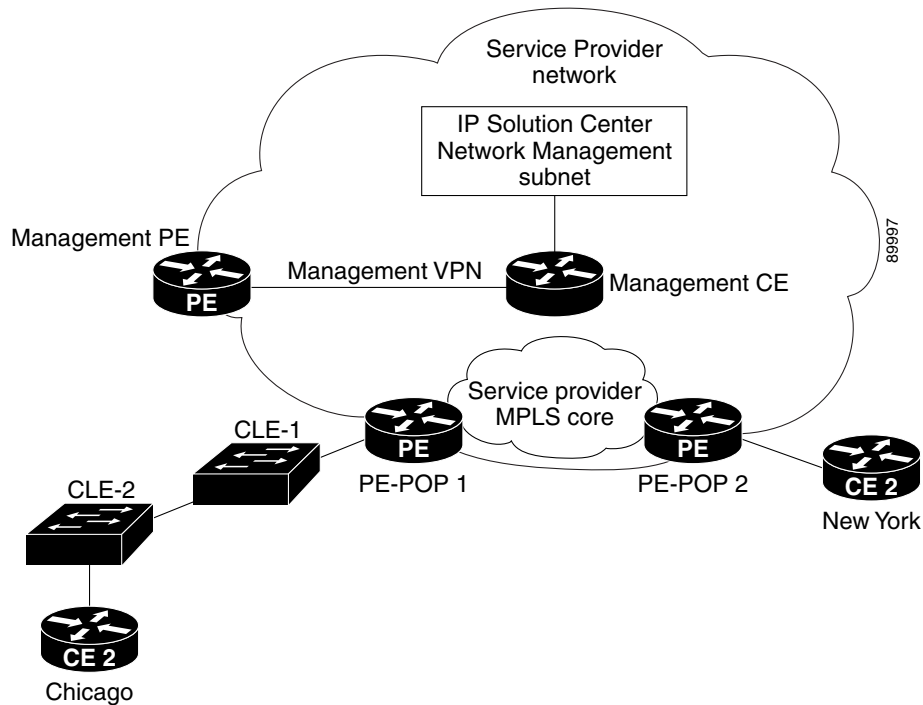
- **VLAN ID Management:** ISC allocates VLAN IDs per customer and per Ethernet Service deployed. The service provider can track per Access Domain a particular allocated VLAN ID (per service or per customer or per Access Domain).

ISC keeps track of the VLANs allocated and gives detailed usage information of the VLAN allocated per service, per customer, or per Access Domain.

*Access Domain:* The Layer 2 Ethernet switching domain attached to a PE defines an *access domain*. All the switches attached to the PE-POP belong to the access domain (as illustrated in Figure A-7). This notion enables the network operator to tie multiple VLAN pools to a single Access Domain, and also allows redundancy with dual PEs in a single Access Domain.

For illustration purpose, let's assume that a Service Provider has a network such as the one illustrated in Figure A-6. A customer has two sites (Chicago and New York), and would like to get an Ethernet Wire Service between the two sites.

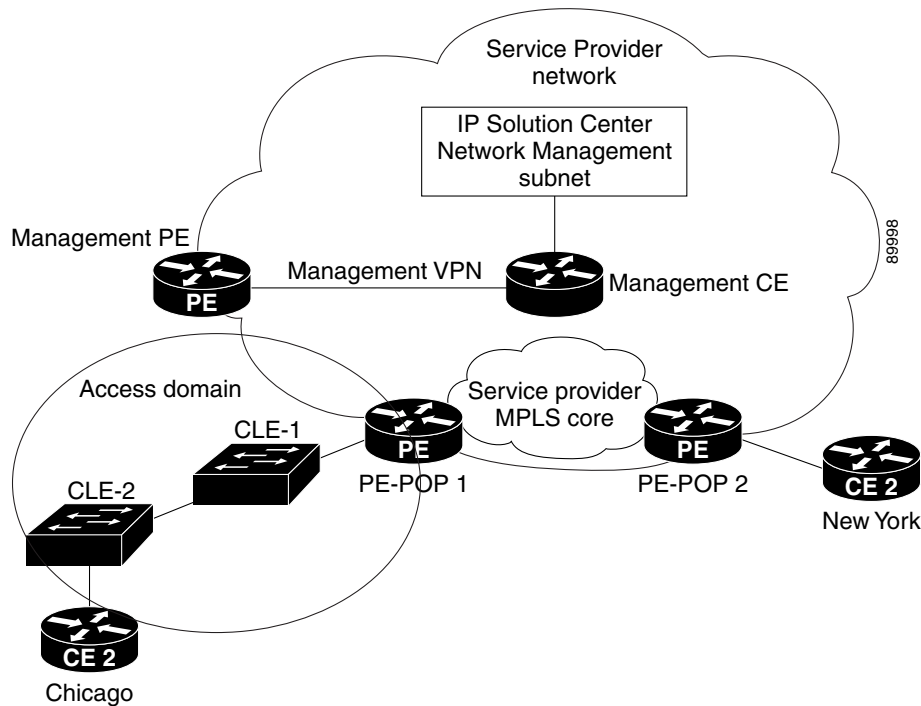
**Figure A-6 Service Provider Network for VLAN ID Management**



1. If the network operator has chosen the **Auto-Pick VLAN ID** option in the service policy (see Specifying PE and CE Interface Parameters, page 5-8), the network operator must assign an access domain and a VLAN pool for a given PE-POP.

This automatically gives ISC the range of VLAN IDs that are attached to the access domain.

Figure A-7 shows the access domain assigned, with PE-POP 1, CLE 1, and CLE 2 defined within the access domain.

**Figure A-7 Access Domain Assigned**

2. All the network elements have been discovered during the Autodiscovery process, and the network topology (connectivity between sites).
3. The service operator wants to deploy an Ethernet over MPLS service from Chicago to New York.
4. Using ISC's GUI, the service operator needs to select the *From* and *To* ports, and the appropriate service policy that allows VLAN IDs in the Access Domain to be picked automatically.
5. ISC allocated a VLAN ID for Chicago and a VLAN ID for New York. (Both sites belong to the same customer.)
6. VLAN IDs are allocated and assigned.

## Resource Pools

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

- *VLAN ID pool*: VLAN ID pools are defined with a starting value and a size of the VLAN pool. A given VLAN ID pool can be attached to an Access Domain. During the deployment an Ethernet Service (EWS, ERS for example), VLAN ID can be auto-allocated from the Access Domain's VLAN pools. This gives the Service Provider a tighter control of VLAN ID allocation.
- *IP address pool*: The IP address pool can be defined and assigned to regions.
- *Multicast pool*: The Multicast pool is used for Multicast MPLS VPNs.
- *Route Target (RT) pool*: A route target is the MPLS mechanism that informs PEs as to which routes should be inserted into the appropriate VRFs. Every VPN route is tagged with one or more route targets when it is exported from a VRF and offered to other VRFs. The route target can be considered a VPN identifier in MPLS VPN architecture. RTs are a 64-bit number.

- *Route Distinguisher (RD) pool*: The IP subnets advertised by the CE routers to the PE routers are augmented with a 64-bit prefix called a route distinguisher (RD) to make them unique. The resulting 96-bit addresses are then exchanged between the PEs, using a special address family of Multiprotocol BGP (referred to as MP-BGP). The RD pool is a pool of 64-bit RD values that ISC uses to make sure the IP addresses in the network are unique.
- *Site of origin pool*: The pool of values for the site-of-origin attribute. The site-of-origin attribute prevents routing loops when a site is multihomed to the MPLS VPN backbone. This is achieved by identifying the site from which the route was learned, based on its SOO value, so that it is not readvertised back to that site from a PE in the MPLS VPN network.

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

## VPN Profile

For all MPLS VPN provisioning, several network elements that participate in the VPN must be defined. These parameters are:

- Choice of protocols between PE-CE and their intrinsic characteristics.
- IP addressing for each site joining the IP VPN
- VRF configuration (export map, import map, maximum number of routes, VRF and RD override, and so forth)
- Choice of joining the VPN as hub or spoke
- Choice of interfaces on the PE, CE, and intermediate network devices

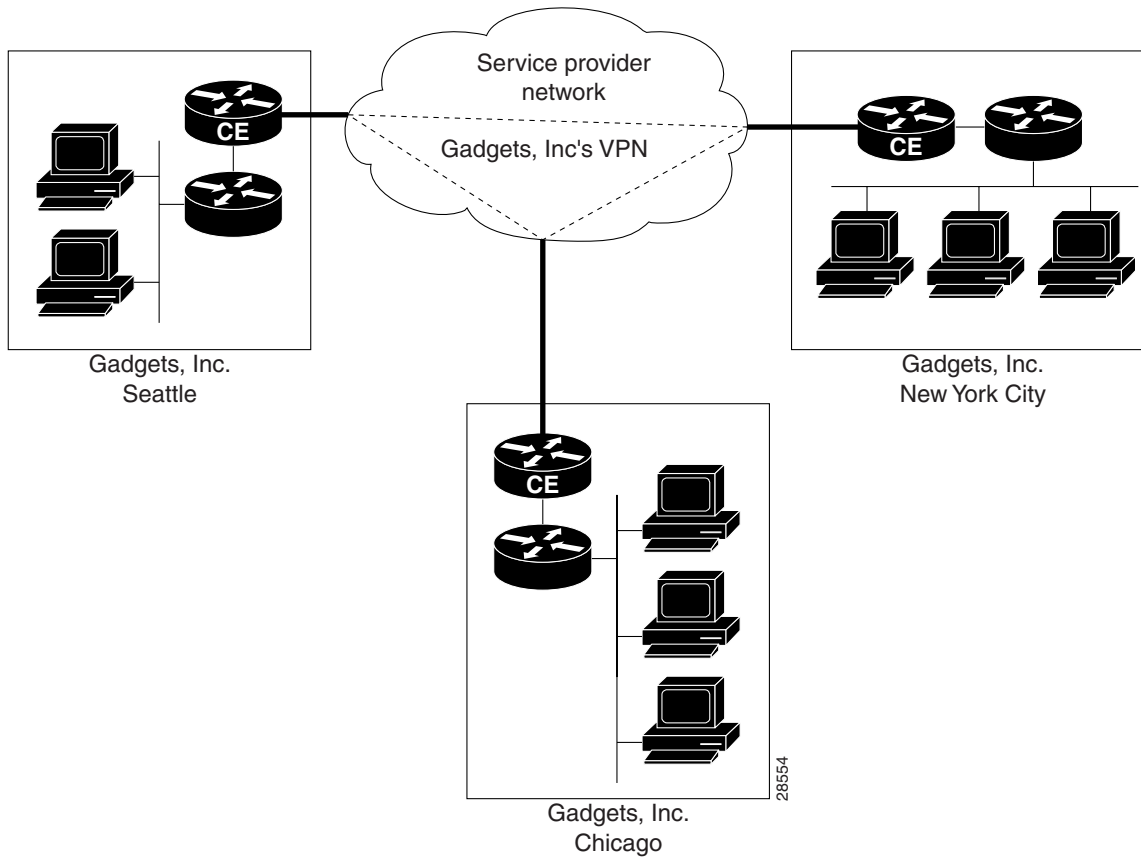
All the provisioning parameters can be made editable for a service operator who will deploy the service. A service policy is defined by a network operator and used by a service operator.

A service policy defines the parameters that will be used during provisioning.

Each of these parameters can be made editable or not to the inexperienced service operator. The fact that a service can be profiled greatly simplifies the service operator's tasks and has now only limited number of parameters to enter during the provisioning process to deploy and activate a MPLS VPN service.

## Customer View

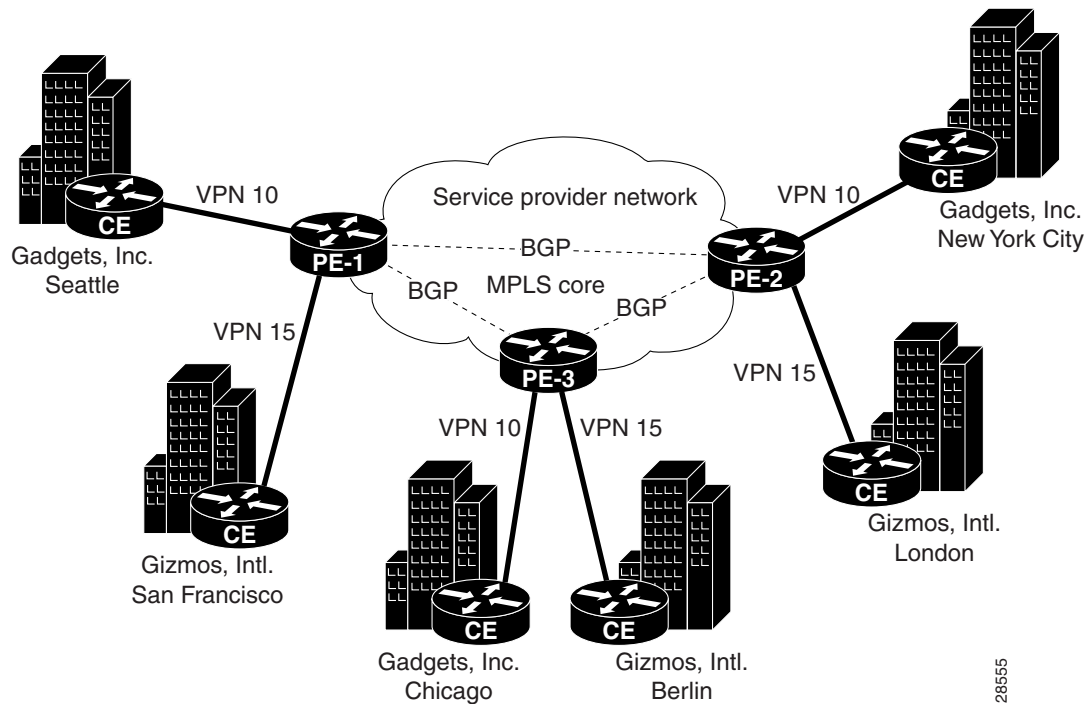
From the customer's point of view, they see their internal routers communicating with their customer edge routers (CEs) from one site to another through a VPN managed by the service provider (see Figure A-8).

**Figure A-8**     *The Customer's View of the Network*

This simple view of the customer's network is the advantage of employing VPNs: the customer experiences direct communication to their sites as though they had their own private network, even though their traffic is traversing a public network infrastructure and they are sharing that infrastructure with other businesses.

## Provider View

The service provider's view of the network is naturally very different, as shown in Figure A-9. This illustration shows two different customers, with each customer having a single VPN. A customer can, however, have multiple VPNs.

**Figure A-9 Service Provider's View of the Network**

## Provider Edge Routers

At the edge of the provider network are provider edge routers (PEs). Within the provider network are other provider routers as needed (often designated as P routers) that communicate with each other and the PEs by way of the Border Gateway Protocol-Multiprotocol (MP-BGP). Note that in this model, the service provider need only provision the links between the PEs and CEs.

PEs maintain separate routing tables called VPN routing and forwarding tables (VRFs). The VRFs contain the routes for directly connected VPN sites only. (For more information about VRFs, see VPN Routing and Forwarding Tables, page A-22). PEs exchange VPN-IPv4 updates through MP-iBGP sessions. These updates contain VPN-IPv4 addresses and labels. The PE originating the route is the next hop of the route. PE addresses are referred to as host routes into the core interior gateway protocol.

## Multi-VRF CE

The Multi-VRF (VPN routing and forwarding tables) CE is a feature that provides for Layer 3 aggregation. Multiple CEs can connect to a single Multi-VRF CE (typically in an enterprise network); then the Multi-VRF CE connects directly to a PE. A Multi-VRF CE can be a Cisco router or a Cisco Catalyst® 3550 Intelligent Ethernet Switch.

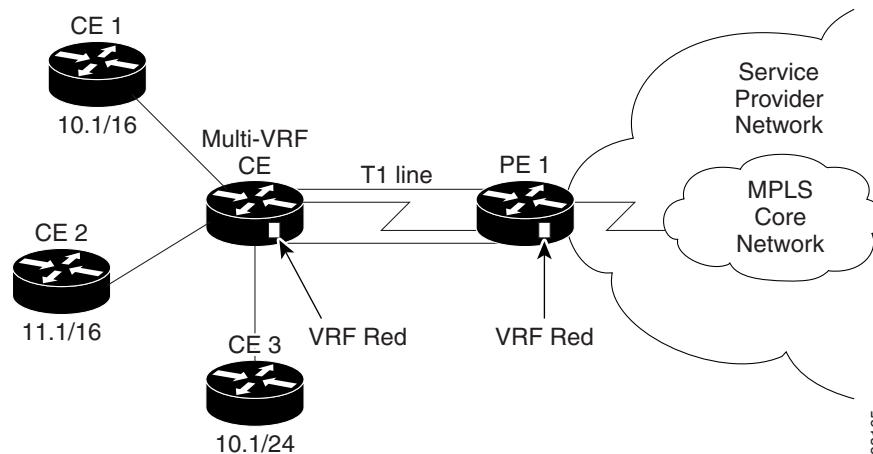
The Multi-VRF CE functionality extends some of the functionality formerly reserved to the PE to a CE router in an MPLS VPN—the only PE-like functionality that this feature provides is the ability to have multiple VRFs on the CE router so that different routing decisions can be made. The packets are sent toward the PE as IP packets.

With this feature, a Multi-VRF CE can maintain separate VRF tables to extend the privacy and security of an MPLS VPN down to a branch office, rather than just at the PE router node.

A Multi-VRF CE is unlike a CE in that there is no label exchange, no LDP adjacency, and no labeled packet flow between the PE and the CE. Multi-VRF CE routers use VRF interfaces to form a VLAN-like configuration on the customer side. Each VRF on the Multi-VRF CE router is mapped to a VRF on the PE router.

Figure A-10 illustrates one method in which a Multi-VRF CE can be used. The Multi-VRF CE router associates a specific VRF by the CEs connected to its interfaces and exchanges that information with the PE. Routes are installed in the VRF on the Multi-VRF CE. There also needs to be a routing protocol or a static route that propagates routes from a specific VRF on the Multi-VRF CE to the corresponding VRF on the PE.

**Figure A-10 A Multi-VRF CE Providing Layer 3 Aggregation**



The Multi-VRF CE feature can segment its LAN traffic by placing each CE with its own IP address space. To differentiate each CE, each interface contains its own IP address space.

When receiving an outbound customer data packet from a directly attached interface, the Multi-VRF CE router performs a route lookup in the VRF that is associated with that site. The specific VRF is determined by the interface or subinterface over which the data packet is received. Support for multiple forwarding tables makes it easy for the Multi-VRF CE router to provide segregation of routing information on a per-VPN basis before the routing information is sent to the PE. The use of a T1 line with multiple point-to-point subinterfaces allows traffic from the Multi-VRF CE router to the PE router to be segmented into each corresponding VRF.

With a Multi-VRF CE, the data path is as follows from the CEs to PE 1 (as shown in Figure A-10):

1. The Multi-VRF CE learns the VPN Red routes to CE 1 from an interface directly attached to the Multi-VRF CE.
2. The Multi-VRF CE then installs these routes into the VRF on the Multi-VRF CE (VRF Red).
3. PE 1 learns the VPN Red routes to CE 1 from the same VRF Red and installs the routes into VRF Red on PE-1.

## Service Audit

A service request audit verifies that service requests are deployed on the network. You can audit new or existing requests. A service request audit can be scheduled on a regular basis to verify the state of the network provisioning requests. The audit verifies the following:

- Verifies the IOS configuration on all network devices.

- Verifies the routing tables and routing for the VPN.

ISC audits against the Repository, not the network. The service operator should schedule auditing after the collection of configuration and routing tables has taken place.

Auditing an existing service request involves three tasks:

- Collects configuration
- Collects routing
- Runs an audit against the specified service requests

### Auditing Report Services

Audit reports provide these services:

- *Audit New Services*: Handles auditing of services requested but not yet deployed (that is, the configuration is not apparent in the router).

The Audit New Services also identifies problems with the download of configuration files to routers

- *Audit Existing Services*: Checks and evaluates configuration of deployed service to see if the service is still in effect.
- *Audit Routing Reports*: Checks the VRF for the VPN on the PE. This report also checks if VPN connectivity is operational by evaluating reachability of the network devices in the VPN.

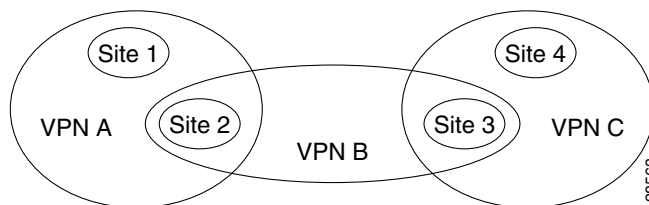
## MPLS VPN

At its simplest, a virtual private network (VPN) is a collection of sites that share the same routing table. A VPN is also a network in which customer connectivity to multiple sites is deployed on a shared infrastructure with the same administrative policies as a private network. The path between two systems in a VPN, and the characteristics of that path, might also be determined (wholly or partially) by policy. Whether a system in a particular VPN is allowed to communicate with systems not in the same VPN is also a matter of policy.

In MPLS VPN, a VPN generally consists of a set of sites that are interconnected by means of an MPLS provider core network, but it is also possible to apply different policies to different systems that are located at the same site. Policies can also be applied to systems that dial in; the chosen policies would be based on the dial-in authentication processes.

A given set of systems can be in one or more VPNs. A VPN can consist of sites (or systems) that are all from the same enterprise (intranet), or from different enterprises (extranet); it might consist of sites (or systems) that all attach to the same service provider backbone, or to different service provider backbones.

**Figure A-11**      **VPNs Sharing Sites**



MPLS-based VPNs are created in Layer 3 and are based on the peer model, which makes them more scalable and easier to build and manage than conventional VPNs. In addition, value-added services, such as application and data hosting, network commerce, and telephony services, can easily be targeted and deployed to a particular MPLS VPN because the service provider backbone recognizes each MPLS VPN as a secure, connectionless IP network.

The MPLS VPN model is a true peer VPN model that enforces traffic separations by assigning unique VPN route forwarding tables (VRFs) to each customer's VPN. Thus, users in a specific VPN cannot see traffic outside their VPN. Traffic separation occurs without tunneling or encryption because it is built directly into the network. (For more information on VRFs, see VPN Routing and Forwarding Tables, page A-22.)

The service provider's backbone is comprised of the PE and its provider routers. MPLS VPN provides the ability that the routing information about a particular VPN be present *only* in those PE routers that attach to that VPN.

### Characteristics of MPLS VPNs

MPLS VPNs have the following characteristics:

- Multiprotocol Border Gateway Protocol-Multiprotocol (MP-BGP) extensions are used to encode customer IPv4 address prefixes into unique VPN-IPv4 Network Layer Reachability Information (NLRI) values.

NLRI refers to a destination address in MP-BGP, so NLRI is considered "one routing unit." In the context of IPv4 MP-BGP, NLRI refers to a network prefix/prefix length pair that is carried in the BGP4 routing updates.

- Extended MP-BGP community attributes are used to control the distribution of customer routes.
- Each customer route is associated with an MPLS label, which is assigned by the provider edge router that originates the route. The label is then employed to direct data packets to the correct egress customer edge router.

When a data packet is forwarded across the provider backbone, two labels are used. The first label directs the packet to the appropriate egress PE; the second label indicates how that egress PE should forward the packet.

- Cisco MPLS CoS and QoS mechanisms provide service differentiation among customer data packets.
- The link between the PE and CE routers uses standard IP forwarding.

The PE associates each CE with a per-site forwarding table that contains only the set of routes available to that CE.

### Principal Technologies

There are four principal technologies that make it possible to build MPLS-based VPNs:

- Multiprotocol Border Gateway Protocol (MP-BGP) between PEs carries CE routing information
- Route filtering based on the VPN route target extended MP-BGP community attribute
- MPLS forwarding carries packets between PEs (across the service provider backbone)
- Each PE has multiple VPN routing and forwarding instances (VRFs)

## Intranets and Extranets

If all the sites in a VPN are owned by the same enterprise, the VPN is a corporate *intranet*. If the various sites in a VPN are owned by different enterprises, the VPN is an *extranet*. A site can be in more than one VPN. Both intranets and extranets are regarded as VPNs.

While the basic unit of connection is the site, the MPLS VPN architecture allows a finer degree of granularity in the control of connectivity. For example, at a given site, it might be desirable to allow only certain specified systems to connect to certain other sites. That is, certain systems at a site might be members of an intranet and members of one or more extranets, while other systems at the same site might be restricted to being members of the intranet only.

A CE router can be in multiple VPNs, although it can only be in a single site. When a CE router is in multiple VPNs, one of these VPNs is considered its primary VPN. In general, a CE router's primary VPN is the intranet that includes the CE router's site. A PE router might attach to CE routers in any number of different sites, whether those CE routers are in the same or in different VPNs. A CE router might, for robustness, attach to multiple PE routers. A PE router attaches to a particular VPN if it is a router adjacent to a CE router that is in that VPN.

## VPN Routing and Forwarding Tables

The VPN routing and forwarding table (VRF) is a key element in the MPLS VPN technology. VRFs exist on PEs only (except in the case of a Multi-VRF CE). A VRF is a routing table instance, and more than one VRF can exist on a PE. A VPN can contain one or more VRFs on a PE. The VRF contains routes that should be available to a particular set of sites. VRFs use Cisco Express Forwarding (CEF) technology, therefore the VPN must be CEF-enabled.

A VRF is associated with the following elements:

- IP routing table
- Derived forwarding table, based on the Cisco Express Forwarding (CEF) technology
- A set of interfaces that use the derived forwarding table
- A set of routing protocols and routing peers that inject information into the VRF

Each PE maintains one or more VRFs. ISC software looks up a particular packet's IP destination address in the appropriate VRF only if that packet arrived directly through an interface that is associated with that VRF. The so-called "color" MPLS label tells the destination PE to check the VRF for the appropriate VPN so that it can deliver the packet to the correct CE and finally to the local host machine.

A VRF is named based on the VPN or VPNs it services, and on the role of the CE in the topology. The schemes for the VRF names are as follows:

The VRF name for a hub: `ip vrf vx:[VPN_name]`

The *x* parameter is a number assigned to make the VRF name unique.

For example, if we consider a VPN called Blue, then a VRF for a hub CE would be called:

```
ip vrf V1:blue
```

A VRF for a spoke CE in the Blue VPN would be called:

```
ip vrf V1:blue-s
```

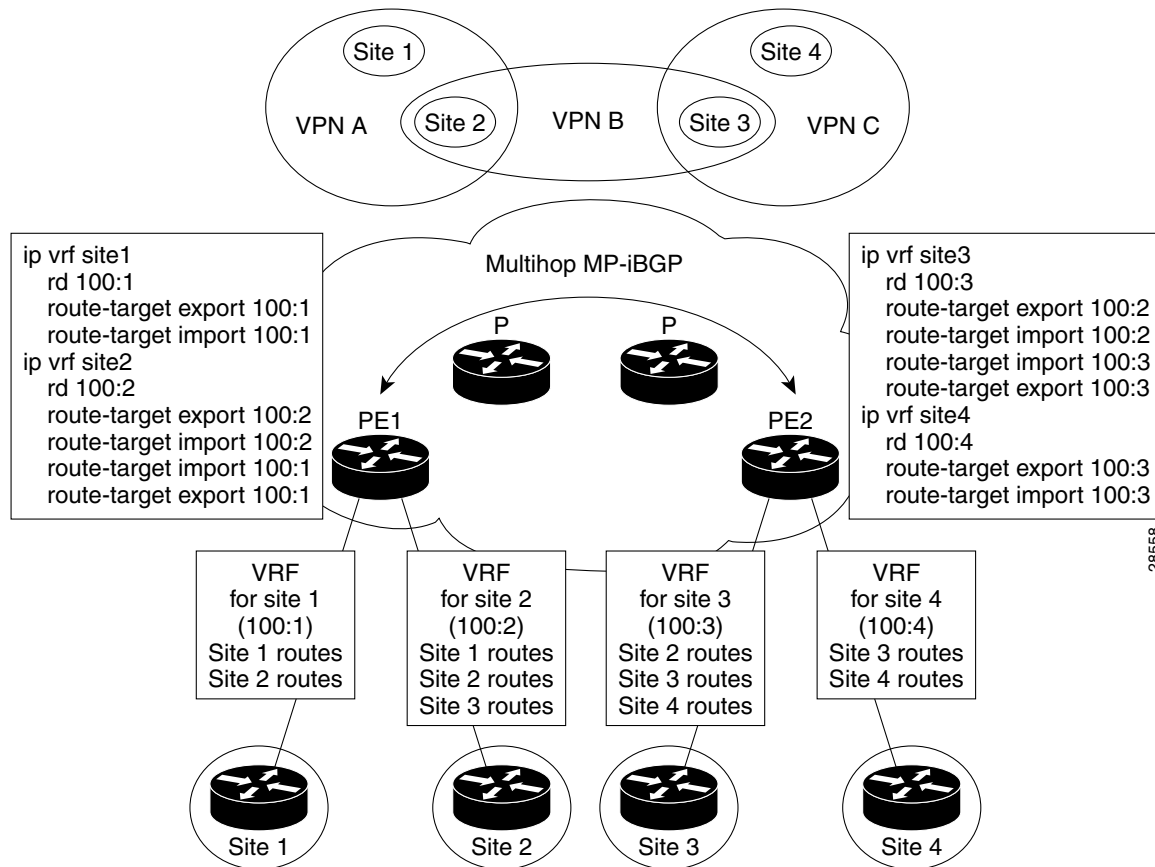
A VRF for an extranet VPN topology in the Green VPN would be called:

```
ip vrf V1:green-etc
```

Thus, you can read the VPN name and the topology type directly from the name of the VRF.

Figure A-12 shows a network in which two of the four sites are members of two VPNs, and illustrates which routes are included in the VRFs for each site.

**Figure A-12** VRFs for Sites in Multiple VPNs



28558

## VRF Implementation

When implementing VPNs and VRFs, Cisco recommends you keep the following considerations in mind:

- A local VRF interface on a PE is not considered a directly-connected interface in a traditional sense. When you configure, for example, a Fast Ethernet interface on a PE to participate in a particular VRF/VPN, the interface no longer shows up as a directly-connected interface when you issue a **show ip route** command. To see that interface in a routing table, you must issue a **show ip route vrf vrf\_name** command.
- The global routing table and the per-VRF routing table are independent entities. Cisco IOS commands apply to IP routing in a global routing table context. For example, **show ip route**, and other EXEC-level show commands—and utilities such as **ping**, **traceroute**, and **telnet**—all invoke the services of the Cisco IOS routines that deal with the global IP routing table.
- You can issue a standard Telnet command from a CE router to connect to a PE router. However, from that PE, you must issue the following command to connect from the PE to the CE:

```
telnet CE_RouterName /vrf vrf_name
```

Similarly, you can utilize the **Traceroute** and **Ping** commands in a VRF context.

- The MPLS VPN backbone relies on the appropriate Interior Gateway Protocol (IGP) that is configured for MPLS, for example, EIGRP, or OSPF. When you issue a **show ip route** command on a PE, you see the IGP-derived routes connecting the PEs together. Contrast that with the **show ip route vrf VRF\_name** command, which displays routes connecting customer sites in a particular VPN.

## VRF Instance

The configuration commands to create a VRF instance are as follows:

	Command	Description
Step 1	Router# <b>configure terminal</b> Router(config)#	Enter global configuration mode.
Step 2	Router(config)# <b>ip vrf vrf_name</b>	For example, <b>ip vrf CustomerA</b> initiates a VPN routing table and an associated CEF table named CustomerA. The command enters VRF configuration submode to configure the variables associated with the VRF.
Step 3	Router(config-vrf)# <b>rd RD_value</b>	Enter the eight-byte route descriptor (RD) or IP address. The PE prepends the RD to the IPv4 routes prior to redistributing the route into the MPLS VPN backbone.
Step 4	Router(config-vrf)# <b>route-target import   export   both community</b>	Enter the route-target information for the VRF.

## Route Distinguishers and Route Targets

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

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

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

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

The route distinguisher values are chosen by the ISC software.

- CEs with hub connectivity use `bgp_AS:value`.
- CEs with spoke connectivity use `bgp_AS:value + 1`

Each spoke uses its own RD value for proper hub and spoke connectivity between CEs; therefore, the ISC software implements a new RD for each spoke that is provisioned.

ISC chooses route target values by default, but you can override the automatically assigned RT values if necessary when you first define a CERC in the ISC software (see *Creating CE Routing Communities*, page 4-6).

## Route Target Communities

The mechanism by which MPLS VPN controls distribution of VPN routing information is through the VPN route-target extended MP-BGP communities. An extended MP-BGP community is an eight octet structure value. MPLS VPN uses route-target communities as follows:

- When a VPN route is injected into MP-BGP, the route is associated with a list of VPN route-target communities. Typically, this is set through an export list of community values associated with the VRF from which the route was learned.
- An import list of route-target communities is associated with each VRF. This list defines the values that should be matched against to decide whether a route is eligible to be imported into this VRF.

For example, if the import list for a particular VRF is {A, B, C}, then any VPN route that carries community value A, B, or C is imported into the VRF.

## CE Routing Communities

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

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

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

These two basic types of VPNs—full mesh and hub and spoke—can be represented with a single CERC.

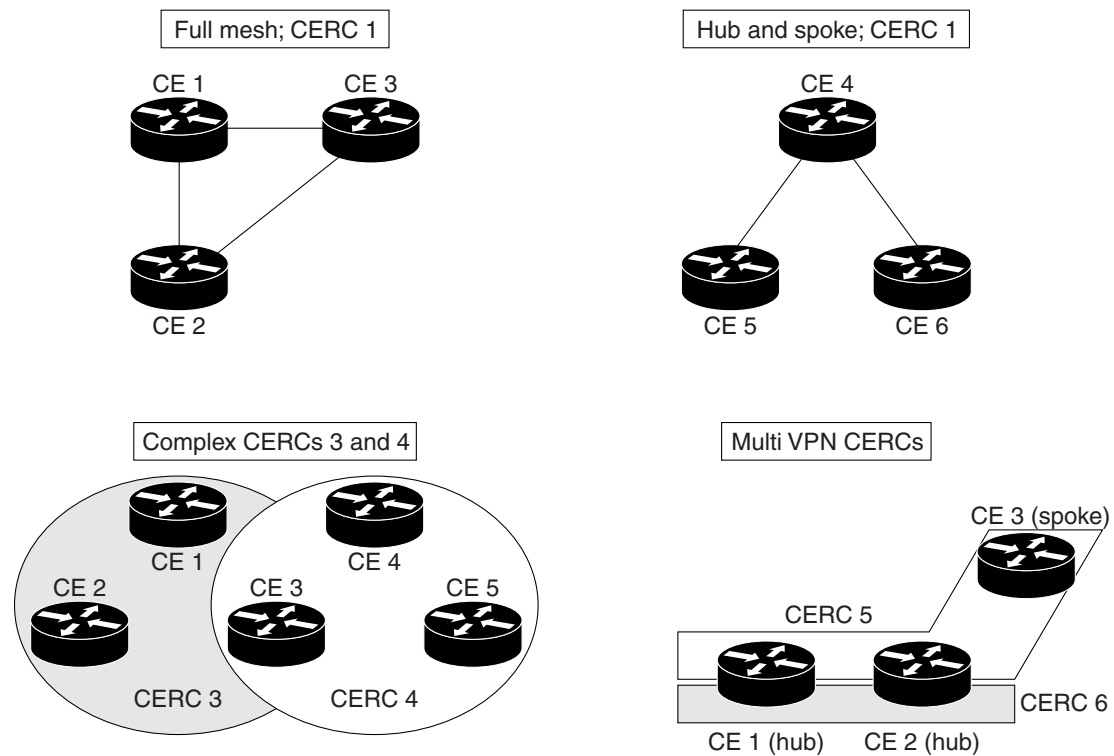
Whenever you create a VPN, the ISC software creates one default CERC for you. This means that until you need advanced customer layout methods, you will not need to define new CERCs. Up to that point, you can think of a CERC as standing for the VPN itself—they are one and the same. If, for any reason, you need to override the software's choice of route target values, you can do so only at the time you create a CERC in the ISC software (see *Creating CE Routing Communities*, page 4-6).

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

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

Figure A-13 shows several examples of the topologies that IP Solution Center CERCs can employ.

**Figure A-13** Examples of CERC Topologies



28902

## Hub and Spoke Considerations

In hub-and-spoke MPLS VPN environments, the spoke routers have to have unique Route Distinguishers (RDs). In order to use the hub site as a transit point for connectivity in such an environment, the spoke sites export their routes to the hub. Spokes can talk to hubs, but spokes never have routes to other spokes.

Due to the current MPLS VPN implementation, you must apply a different RD for each spoke VRF. The MP-BGP selection process applies to all the routes that have to be imported into the same VRF plus all routes that have the same RD of such a VRF. Once the selection process is done, only the best routes are imported. In this case this can result in a best route which is not imported. Thus, customers must have different RDs per spoke-VRF.

## Full Mesh Considerations

Each CE Routing Community (CERC) has two distinct RTs: a hub RT and a spoke RT. When building a full mesh topology, always use the hub RT. Thus, when a need arises to add a spoke site for the current full mesh topology, you can easily add the spoke site without reconfiguring any of the hub sites. The existing spoke RT can be used for this purpose. This is a strategy to prevent having to do significant reprovisioning of a full mesh topology to a hub-and-spoke topology.

# MPLS VPN Security

This section discusses the security requirements for MPLS VPN architectures. This section concentrates on protecting the core network against attacks from the “outside,” that is, the Internet and connected VPNs. Protection against attacks from the “inside,” that is, when an attacker has logical or physical access to the core network is not discussed here, since any network can be attacked with access from the inside.

## Address Space and Routing Separation

Between two non-intersecting VPNs of an MPLS VPN service, it is assumed that the address space between different VPNs is entirely independent. This means, for example, that two non-intersecting VPNs must be able to both use the 10/8 network without any interference. From a routing perspective, this means that each end system in a VPN has a unique address, and all routes to this address point to the same end system. Specifically:

- Any VPN must be able to use the same address space as any other VPN.
- Any VPN must be able to use the same address space as the MPLS core.
- Routing between any two VPNs must be independent.
- Routing between any VPN and the core must be independent.

## Address Space Separation

From a security point of view, the basic requirement is to avoid that packets destined to a host a.b.c.d within a given VPN reach a host with the same address in another VPN or the core.

MPLS allows distinct VPNs to use the same address space, which can also be private address space. This is achieved by adding a 64-bit route distinguisher (RD) to each IPv4 route, making VPN-unique addresses also unique in the MPLS core. This “extended” address is also called a *VPN-IPv4 address*. Thus customers of an MPLS service do not need to change current addressing in their networks.

In the case of using routing protocols between CE and PE routers (for static routing this is not an issue), there is one exception—the IP addresses of the PE routers the CE routers are peering with. To be able to communicate to the PE router, routing protocols on the CE routers must configure the address of the peer router in the core. This address must be unique from the CE router’s perspective. In an environment where the service provider manages also the CE routers as CPE (customer premises equipment), this can be made invisible to the customer.

## Routing Separation

Routing separation between the VPNs can also be achieved. Every PE router maintains a separate Virtual Routing and Forwarding instance (VRF) for each connected VPN. Each VRF on the PE router is populated with routes from one VPN, through statically configured routes or through routing protocols that run between the PE and the CE router. Since every VPN results in a separate VRF, there are no interferences between the VPNs on the PE router.

Across the MPLS core to the other PE routers, this routing separation is maintained by adding unique VPN identifiers in multi-protocol BGP, such as the route distinguisher (RD). VPN routes are exclusively exchanged by MP-BGP across the core, and this BGP information is not redistributed to the core network, but only to the other PE routers, where the information is kept again in VPN-specific VRFs. Thus routing across an MPLS network is separate per VPN.

Given addressing and routing separation across an MPLS core network, MPLS offers in this respect the same security as comparable Layer 2 VPNs, such as ATM or Frame Relay. It is not possible to intrude into other VPNs through the MPLS core, unless this has been configured specifically.

## Hiding the MPLS Core Structure

The internal structure of the MPLS core network (PE and Provider router devices) should not be visible to outside networks (either the Internet or any connected VPN). While a breach of this requirement does not lead to a security problem itself, it is generally advantageous when the internal addressing and network structure remains hidden to the outside world. The ideal is to not reveal any information of the internal network to the outside. This applies equally to the customer networks as to the MPLS core.

Denial-of-service attacks against a core router, for example, are much easier to carry out if an attacker knows the IP address. Where addresses are not known, they can be guessed, but when the MPLS core structure is hidden, attacks are more difficult to make. Ideally, the MPLS core should be as invisible to the outside world as a comparable Layer 2 infrastructure (for example, Frame Relay or ATM).

In practice, a number of additional security measures have to be taken, most of all *extensive packet filtering*. MPLS does not reveal unnecessary information to the outside, not even to customer VPNs. The addressing in the core can be done with either private addresses or public addresses. Since the interface to the VPNs, and potentially to the Internet, is BGP, there is no need to reveal any internal information. The only information required in the case of a routing protocol between a PE and CE is the address of the PE router. If this is not desired, you can configure static routing between the PE and CE. With this measure, the MPLS core can be kept completely hidden.

To ensure reachability across the MPLS cloud, customer VPNs will have to advertise their routes as a minimum to the MPLS core. While this could be seen as too open, the information known to the MPLS core is not about specific hosts, but networks (routes); this offers some degree of abstraction. Also, in a VPN-only MPLS network (that is, no shared Internet access), this is equal to existing Layer 2 models, where the customer has to trust the service provider to some degree. Also in a Frame Relay or ATM network, routing information about the VPNs can be seen on the core network.

In a VPN service with shared Internet access, the service provider typically announces the routes of customers that wish to use the Internet to his upstream or peer providers. This can be done by way of a network address translation (NAT) function to further obscure the addressing information of the customers' networks. In this case, the customer does not reveal more information to the general Internet than with a general Internet service. Core information is not revealed at all, except for the peering addresses of the PE router) that hold the peering with the Internet. - **NAT is not supported in this release.** -

In summary, in a pure MPLS VPN service, where no Internet access is provided, the level of information hiding is as good as on a comparable Frame Relay or ATM network—no addressing information is revealed to third parties or the Internet. If a customer chooses to access the Internet by way of the MPLS core, he will have to reveal the same addressing structure as for a normal Internet service. NAT can be used for further address hiding. - **NAT is not supported in this release.** -

If an MPLS network has no interconnections to the Internet, this is equal to Frame Relay or ATM networks. With Internet access from the MPLS cloud, the service provider has to reveal at least one IP address (of the peering PE router) to the next provider, and thus the outside world.

## Resistance to Attacks

It is not possible to directly intrude into other VPNs. However, it is possible to attack the MPLS core, and try to attack other VPNs from there. There are two basic ways the MPLS core can be attacked:

- Attacking the PE routers directly.
- Attacking the signaling mechanisms of MPLS (mostly routing)

There are two basic types of attacks: *denial-of-service (DoS) attacks*, where resources become unavailable to authorized users, and *intrusion attacks*, where the goal is to gain unauthorized access to resources.

For intrusion attacks, give unauthorized access to resources, there are two basic ways to protect the network:

- Harden protocols that could be abused (for example, Telnet to a router)
- Make the network as inaccessible as possible. This is achieved by a combination of filtering packets or employing firewalls and hiding the IP addresses in the MPLS core. - **Firewall is not supported in this release.** -

Denial-of service attacks are easier to execute, since in the simplest case, a known IP address might be enough to attack a machine. The only way to be certain that you are not be vulnerable to this kind of attack is to make sure that machines are not reachable, again by packet filtering and pinging IP addresses.

MPLS networks must provide at least the same level of protection against both forms of attack as current Layer 2 networks provide.

To attack an element of an MPLS network it is first necessary to know this element, that is, its IP address. It is possible to hide the addressing structure of the MPLS core to the outside world, as discussed in the previous section. Thus, an attacker does not know the IP address of any router in the core that he wants to attack. The attacker could guess addresses and send packets to these addresses. However, due to the address separation of MPLS, each incoming packet is treated as belonging to the address space of the customer. It is therefore impossible to reach an internal router, even through guessing the IP addresses. There is only one exception to this rule—the peer interface of the PE router.

## Securing the Routing Protocol

The routing between the VPN and the MPLS core can be configured two ways:

1. **Static.** In this case, the PE routers are configured with static routes to the networks behind each CE, and the CEs are configured to statically point to the PE router for any network in other parts of the VPN (usually a default route).

The static route can point to the IP address of the PE router, or to an interface of the CE router (for example, serial0).

Although in the static case the CE router does not know any IP addresses of the PE router, it is still attached to the PE router by way of some method, and could guess the address of the PE router and try to attack it with this address.

In the case of a static route from the CE router to the PE router, which points to an interface, the CE router does not need to know any IP address of the core network, not even of the PE router. This has the disadvantage of a more extensive (static) configuration, but from a security point of view, it is preferable to the other cases.

2. **Dynamic.** A routing protocol (for example, RIP, OSPF, or BGP) is used to exchange the routing information between the CE and the PE at each peering point.

In all other cases, each CE router needs to know at least the router ID (RID; peer IP address) of the PE router in the MPLS core, and thus has a potential destination for an attack.

In practice, access to the PE router over the CE-PE interface can be limited to the required routing protocol by using access control lists (ACLs). This limits the point of attack to one routing protocol, for example BGP. A potential attack could send an extensive number of routes, or flood the PE router with routing updates. Both of these attacks could lead to a denial-of-service attack, however, not to an intrusion attack.

To restrict this risk it is necessary to configure the routing protocol on the PE router as securely as possible. This can be done in various ways:

- Use VRFs. There are mechanisms within the context of a VRF for a service provider to monitor and control the number of routes that a customer can have in the VPN. When such thresholds are breached, for example 80 percent of the allowed number of routes syslog messages can be generated indicating to the service provider that the VRF is reaching the allowed limit.
- Use ACLs. Allow the routing protocol only from the CE router, not from anywhere else. Furthermore, no access other than that should be allowed to the PE router in the inbound ACL on each PE interface.

ACLs must be configured to limit access only to the port(s) of the routing protocol, and only from the CE router.

- Where available, configure MD-5 authentication for routing protocols.

This is available for BGP, OSPF, and RIP2. It avoids the possibility that packets could be spoofed from other parts of the customer network than the CE router. This requires that the service provider and customer agree on a shared secret between all CE and PE routers. The problem here is that it is necessary to do this for all VPN customers; it is not sufficient to do this only for the customer with the highest security requirements.

**Note**

ISC does not provide for the provisioning of MD5 authentication on PE-CE links using routing protocols. The VPN customer and the service provider must manually configure this.

MD5 authentication in routing protocols should be used on all PE-CE peers. It is easy to track the source of such a potential denial-of-service attack.

- Configure, where available, the parameters of the routing protocol to further secure this communication.

In BGP, for example, it is possible to configure *dampening*, which limits the number of routing interactions. Also, a maximum number of routes accepted per VRF should be configured where possible.

In summary, it is not possible to intrude from one VPN into other VPNs or the core. However, it is theoretically possible to exploit the routing protocol to execute a denial-of-service attack against the PE router. This in turn might have negative impact on other VPNs. For this reason, PE routers must be extremely well secured, especially on their interfaces to the CE routers.

## Label Spoofing

Assuming the address and routing separation as discussed above, a potential attacker might try to gain access to other VPNs by inserting packets with a label that he does not own. This is called *label spoofing*. This kind of attack can be done from the outside, that is, another CE router or from the Internet, or from within the MPLS core. The latter case (from within the core) is not discussed since the assumption is that the core network is provided in a secure manner. Should protection against an insecure core be required, it is necessary to run IPsec on top of the MPLS infrastructure. - **Ipsec is not supported in this release.** -

Within the MPLS network, packets are not forwarded based on the IP destination address, but based on the labels that are prepended by the PE routers. Similar to IP spoofing attacks, where an attacker replaces the source or destination IP address of a packet, it is also possible to spoof the label of an MPLS packet.

The interface between any CE router and its peering PE router is an IP interface, that is, without labels. The CE router is unaware of the MPLS core, and is only aware of the destination router. The intelligence exists in the PE device, where based on the configuration, the PE chooses a label and prepends it to the packet. This is the case for all PE routers, toward CE routers, and to the upstream service provider. All interfaces into the MPLS cloud require IP packets without labels.

For security reasons, a PE router should never accept a packet with a label from a CE router. Cisco routers implementation is such that packets that arrive on a CE interface with a label are dropped. Thus, it is not possible to insert fake labels because no labels are accepted. Additional security can be implemented by using MD5 authentication between peer routers in the core if the service provider is using LDP to distribute labels.

There remains the possibility to spoof the IP address of a packet that is being sent to the MPLS core. However, since there is strict addressing separation within the PE router, and each VPN has its own VRF, this can only do harm to the VPN the spoofed packet originated from, in other words, a VPN customer can attack himself. MPLS does not add any security risk here.

## Securing the MPLS Core

The following is a list of recommendations and considerations on configuring an MPLS network securely.



### Note

The security of the overall solution depends on the security of its weakest link. This could be the weakest single interconnection between a PE and a CE, an insecure access server, or an insecure TFTP server.

## Trusted Devices

The PE and P devices, and remote access servers and AAA servers must be treated as trusted systems. This requires strong security management, starting with physical building security and including issues such as access control, secure configuration management, and storage. There is ample literature available on how to secure network elements, so these topics are not discussed here in more detail.

CE routers are typically not under full control of the service provider and must be treated as “untrusted.”

## PE-CE Interface

The interface between PE and CE routers is crucial for a secure MPLS network. The PE router should be configured as close as possible. From a security point of view, the best option is to configure the interface to the CE router unnumbered and route statically.

Packet filters (Access Control Lists) should be configured to permit only one specific routing protocol to the peering interface of the PE router, and only from the CE router. All other traffic to the router and the internal service provider network should be denied. This avoids the possibility that the PE and P routers can be attacked, since all packets to the corresponding address range are dropped by the PE router. The only exception is the peer interface on the PE router for routing purposes. This PE peer interface must be secured separately.

If private address space is used for the PE and P routers, the same rules with regard to packet filtering apply—it is required to filter all packets to this range. However, since addresses of this range should not be routed over the Internet, it limits attacks to adjacent networks.

## Routing Authentication

All routing protocols should be configured with the corresponding authentication option toward the CEs and toward any Internet connection. Specifically: BGP, OSPF, and RIP2. All peering relationships in the network need to be secured this way:

- CE-PE link: use BGP MD-5 authentication
- PE-P link: use LDP MD5 authentication
- P-P

This prevents attackers from spoofing a peer router and introducing bogus routing information. Secure management is particularly important regarding configuration files, which often contain shared secrets in clear text (for example for routing protocol authentication).

## Separation of CE-PE Links

If several CEs share a common Layer 2 infrastructure to access the same PE router (for example, an ethernet VLAN), a CE router can spoof packets as belonging to another VPN that also has a connection to this PE router. Securing the routing protocol is not sufficient, since this does not affect normal packets.

To avoid this problem, Cisco recommends that you implement separate physical connections between CEs and PEs. The use of a switch between various CE routers and a PE router is also possible, but it is strongly recommended to put each CE-PE pair into a separate VLAN to provide traffic separation. Although switches with VLANs increase security, they are not unbreakable. A switch in this environment must thus be treated as a trusted device and configured with maximum security.

## LDP Authentication

The Label Distribution Protocol (LDP) can also be secured with MD-5 authentication across the MPLS cloud. This prevents hackers from introducing bogus routers, which would participate in the LDP.

## Connectivity Between VPNs

MPLS provides VPN services with address and routing separation between VPNs. In many environments, however, the devices in the VPN must be able to reach destinations outside the VPN. This could be for Internet access or for merging two VPNs, for example, in the case of two companies merging. MPLS not only provides full VPN separation, but also allows merging VPNs and accessing the Internet.

To achieve this, the PE routers maintain various tables: A *routing context table* is specific to a CE router, and contains only routes from this particular VPN. From there, routes are propagated into the *VRF* (virtual routing and forwarding instance) *routing table*, from which a *VRF forwarding table* is calculated.

For separated VPNs, the VRF routing table contains only routes from one routing context. To merge VPNs, different routing contexts (from different VPNs) are put into one single VRF routing table. In this way, two or several VPNs can be merged to a single VPN. In this case, it is necessary that all merged VPNs have mutually exclusive addressing spaces; in other words, the overall address space must be unique for all included VPNs.

For a VPN to have Internet connectivity, the same procedure is used: Routes from the Internet VRF routing table (the default routing table) are propagated into the VRF routing table of the VPN that requires Internet access. Alternatively to propagating all Internet routes, a default route can be propagated. In this case, the address space between the VPN and the Internet must be distinct. The VPN must use private address space since all other addresses can occur in the Internet.

From a security point of view, the merged VPNs behave like one logical VPN, and the security mechanisms described above apply now between the merged VPN and other VPNs. The merged VPN must have unique address space internally, but further VPNs can use the same address space without interference. Packets from and to the merged VPNs cannot be routed to other VPNs. All the separation functions of MPLS apply also for merged VPNs with respect to other VPNs.

If two VPNs are merged in this way, hosts from either part can reach the other part as if the two VPNs were a common VPN. With the standard MPLS features, there is no separation or firewalling or packet filtering between the merged VPNs. Also, if a VPN receives Internet routes through MPLS/BGP VPN mechanisms, firewalling or packet filtering has to be engineered in addition to the MPLS features. -

**Firewall is not supported in this release. -**

## MP-BGP Security Features

Security in ISC MPLS-based networks is delivered through a combination of MP-BGP and IP address resolution. In addition, service providers can ensure that VPNs are isolated from each other.

Multiprotocol BGP is a routing information distribution protocol that, through employing multiprotocol extensions and community attributes, defines who can talk to whom. VPN membership depends upon logical ports entering the VPN, where MP-BGP assigns a unique Route Distinguisher (RD) value (see Route Distinguishers and Route Targets, page A-24).

RDs are unknown to end users, making it impossible to enter the network on another access port and spoof a flow. Only preassigned ports are allowed to participate in the VPN. In an MPLS VPN, MP-BGP distributes forwarding information base (FIB) tables about VPNs to members of the same VPN only, providing native security by way of logical VPN traffic separation. Furthermore, IBGP PE routing peers can perform TCP segment protection using the MD5 Signature Option when establishing IBGP peering relationships, further reducing the likelihood of introducing spoofed TCP segments into the IBGP connection stream among PE routers (for information on the MD5 Signature Option, see RFC 2385).

The service provider, not the customer, associates a specific VPN with each interface when provisioning the VPN. Users can only participate in an intranet or extranet if they reside on the correct physical or logical port and have the proper RD. This setup makes a Cisco MPLS VPN virtually impossible to enter.

Within the core, a standard Interior Gateway Protocol (IGP) such as OSPF or IS-IS distributes routing information. Provider edge routers set up paths among one another using LDP to communicate label-binding information. Label binding information for external (customer) routes is distributed among PE routers using MP-BGP multiprotocol extensions instead of LDP, because they easily attach to VPN IP information already being distributed.

The MP-BGP community attribute constrains the scope of reachability information. MP-BGP maps FIB tables to provider edge routers belonging to only a particular VPN, instead of updating all edge routers in the service provider network.

## Security Through IP Address Resolution

MPLS VPN networks are easier to integrate with IP-based customer networks. Subscribers can seamlessly interconnect with a provider service without changing their intranet applications because MPLS-based networks have built-in application awareness. Customers can even transparently use their existing IP address space without Network Address Translator (NAT) because each VPN has a unique identifier. - **NAT is not supported in this release.** -

MPLS VPNs remain unaware of one another. Traffic is separated among VPNs using a logically distinct forwarding table and RD for each VPN. Based on the incoming interface, the PE selects a specific forwarding table, which lists only valid destinations in the VPN. To create extranets, a provider explicitly configures reachability among VPNs.

The forwarding table for a PE contains only address entries for members of the same VPN. The PE rejects requests for addresses not listed in its forwarding table. By implementing a logically separate forwarding table for each VPN, each VPN itself becomes a private, connectionless network built on a shared infrastructure.

IP limits the size of an address to 32 bits in the packet header. The VPN IP address adds 64 bits in front of the header, creating an extended address in routing tables that classical IP cannot forward. The extra 64 bits are defined by the Route Distinguisher and the resultant route becomes a unique 96-bit prefix. MPLS solves this problem by forwarding traffic based on labels, so one can use MPLS to bind VPN IP routes to label-switched paths. PEs are concerned with reading labels, not packet headers. MPLS manages forwarding through the provider's MPLS core. Since labels only exist for valid destinations, this is how MPLS delivers both security and scalability.

When a virtual circuit is provided using the overlay model, the egress interface for any particular data packet is a function solely of the packet's ingress interface; the IP destination address of the packet does not determine its path in the backbone network. Thus, unauthorized communication into or out of a VPN is prevented.

In MPLS VPNs, a packet received by the backbone is first associated with a particular VPN by stipulating that all packets received on a certain interface (or subinterface) belong to a certain VPN. Then its IP address is looked up in the forwarding table associated with that VPN. The routes in that forwarding table are specific to the VPN of the received packet.

In this way, the ingress interface determines a set of possible egress interfaces, and the packet's IP destination address is used to choose from among that set. This prevents unauthorized communication into and out of a VPN.

## Ensuring VPN Isolation

To maintain proper isolation of one VPN from another, it is important that the provider routers not accept a labeled packet from any adjacent PE unless the following conditions are met:

- The label at the top of the label stack was actually distributed by the provider router to the PE device.
- The provider router can determine that use of that label will cause the packet to exit the backbone before any labels lower in the stack and the IP header will be inspected.

These restrictions are necessary to prevent packets from entering a VPN where they do not belong.

The VRF tables in a PE are used only for packets arriving from a CE that is directly attached to the PE device. They are not used for routing packets arriving from other routers that belong to the service provider backbone. As a result, there might be multiple different routes to the same system, where the route followed by a given packet is determined by the site from which the packet enters the backbone.

So one might have one route to a given IP network for packets from the extranet (where the route leads to a firewall), and a different route to the same network for packets from the intranet. - **Firewall is not supported in this release.** -





## Service Request Transition States

Table B-1 and Table B-2 on page B-2 show the state transition paths for IP Solution Center (ISC) service requests. The beginning state of a service request is listed in the first column; the states that service requests transition to are displayed in the heading row.

For example, to use Table B-1 to trace the state of a Pending service request to Functional, find **Pending** in the first column and move to your right until you find **Functional** in the heading. You can see that for a service request to move from Pending to Functional, a successful routing audit must take place.

Table B-1 shows the service request transitions from *Requested* to *Lost*.

**Table B-1**      **State Transition Paths for ISC Service Requests (Part 1)**

<b>Service Request States</b>	<b>Requested</b>	<b>Pending</b>	<b>Failed Audit</b>	<b>Deployed</b>	<b>Functional</b>	<b>Lost</b>
<b>Requested</b>	No transition to Requested	Successful service request deployment	No transition to Failed Audit	No transition to Deployed	No transition to Functional	No transition to Lost
<b>Pending</b>	No transition to Requested	Successful service request deployment	Audit is not successful	Audit is successful	Routing audit is successful	No transition to Lost
<b>Failed Audit</b>	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	No transition to Lost
<b>Deployed</b>	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	Audit found error
<b>Functional</b>	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	No transition to Deployed	Routing audit is successful	Audit found error
<b>Lost</b>	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	Audit found error
<b>Broken</b>	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	No transition to Deployed	Routing audit is successful	Audit found error

**Table B-1 State Transition Paths for ISC Service Requests (Part 1) (continued)**

Service Request States	Requested	Pending	Failed Audit	Deployed	Functional	Lost
<b>Invalid</b>	No transition to Requested	Successful service request redeployment	Redeployment caused service request error	No transition to Deployed	No transition to Functional	No transition to Lost
<b>Failed Deploy</b>	No transition to Requested	Successful service request redeployment	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Deployed	No transition to Functional	No transition to Lost
<b>Closed</b>	No transition to Requested	No transition to Pending	No transition to Failed Audit	No transition to Deployed	No transition to Functional	No transition to Lost

Table B-2 shows the service request transitions from *Broken* to *Closed*.

**Table B-2 State Transition Paths for ISC Service Requests (Part 2)**

Service Request States	Broken	Invalid	Failed Deploy	Closed
<b>Requested</b>	No transition to Broken	Deploy Service Request error	Deployment failed	No transition to Closed
<b>Pending</b>	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	Removal of the service request is successful
<b>Failed Audit</b>	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
<b>Deployed</b>	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
<b>Functional</b>	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
<b>Lost</b>	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
<b>Broken</b>	Route audit is not successful. Configlet is correct.	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
<b>Invalid</b>	No transition to Broken	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed

**Table B-2**      *State Transition Paths for ISC Service Requests (Part 2) (continued)*

<b>Service Request States</b>	<b>Broken</b>	<b>Invalid</b>	<b>Failed Deploy</b>	<b>Closed</b>
<b>Failed Deploy</b>	No transition to Broken	Redeploy service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
<b>Closed</b>	No transition to Broken	No transition to Invalid	No transition to Failed Deploy	No transition to Closed





## Troubleshooting MPLS VPN

---

This chapter contains the following major sections:

- MPLS VPN Provisioning Workflow, page C-1
- General Troubleshooting Guidelines, page C-2
- Common Provisioning Issues, page C-2
- Troubleshooting MPLS VPN and Layer 2 VPN, page C-4

### MPLS VPN Provisioning Workflow

The tasks listed below depict the MPLS provisioning workflow. This section assumes an operator deploys a service request using a caller such as Task Manager.

1. The Provisioning driver (ProvDrv) gets the service request to be deployed.
2. From the service request, the Provisioning driver deduces which devices are involved.
3. The latest router configurations must be obtained, so the Provisioning driver tells the Generic Transport Library (GTL)/ Device Configuration Service (DCS) to upload the latest router configurations. The result is used by the service module.
4. The Provisioning driver determines what service modules are involved based on the service and device types.
5. The Provisioning driver queries the Repository for the service intention. The Provisioning driver sends the service intention to the service module, along with the uploaded configuration.
6. The service module generates configlets based on the configurations and service intention and returns the appropriate configlets to the Provisioning driver.
7. The Provisioning driver signals GTL/DCS to download the configlets to the target routers.
8. The Provisioning driver sends the updated result, including the download result, to the Repository, which then updates its state.

## Terms Defined

- **Device Configuration Service (DCS):** Responsible for uploading and downloading configuration files.
- **Generic Transport Library:** Provides APIs for downloading configlets to target devices, uploading configuration files from target devices, executing commands on target devices, and reloading the target device.

This library provides a layer between the transport provider (DCS) and the client application (for example, the Provisioning Driver, Auditor, Collect Config operation, Exec command). The main role of the GTL is to collect the target specific information from the Repositories and the *properties* file and pass it on to the transport provider (DCS).

- **ProvDrv (the Provisioning driver):** ProvDrv is the task responsible for deploying one or more services on multiple devices.

ProvDrv performs the tasks that are common to all services, such as the just-in-time upload of configuration files from the devices, invocation of the Data Driven Provisioning (DDP) engine, obtaining the generated configlets or the audit reports from the DDP engine, and downloading the configlets to the devices.

- **Repository:** The Repository houses various IP Solution Center data. The ISC Repository uses Sybase or Oracle.
- **Service module:** Generates configlets based on the service types.

## General Troubleshooting Guidelines

For general troubleshooting of failed provisioning, follow these steps:

- 
- Step 1** Identify the failed service request and go into **Details**.
- To do this, go to the Service Request Editor and click **Details**. Of main concern is the status message—this tells you exactly what happened.
  - If the status message tells you it's a failed audit, click the **Audit** button to find out exactly what part of the audit failed.
- Step 2** If the troubleshooting sequence in Step 1 doesn't give you a clear idea as to what happened, use the logs in the Task Manager to identify the problem.
- To do this, choose **Monitoring > Task Manager > Logs > Task Name**.
  - There is a lot of information in this log. To isolate the problem, you can use the filter. If you filter by log level and/or component, you can usually reduce the amount of irrelevant information and focus on the information you must know to locate the problem.
- 

## Common Provisioning Issues

Below is a list of common provisioning problems and recommended solutions.

**Symptom 1**

My task does not execute even if I schedule it for immediate deployment.

**Recommended Action**

This problem is likely due to one of the ISC servers being stopped or disabled.

- Step 1** To check the status of all ISC servers, open the Host Configuration dialog by choosing **Administration > Control Center**.  
The Control Center Hosts page is displayed.
- Step 2** Click the check box for the host of interest.  
The menu buttons for the Hosts page are enabled.
- Step 3** Select **Servers**.  
The Server Status page is displayed (see Figure C-1).

**Figure C-1** ISC Server Status

Servers								
								Refresh
Showing 1 - 9 of 9 records								
#	<input type="checkbox"/>	Name	State	Generation	Start Time	PID	Successful Heartbeats	Missed Heartbeats
1.	<input type="checkbox"/>	cornerstonebridge	started	1	Feb 07 12:54:42 PM PST	13774	3750	0
2.	<input type="checkbox"/>	worker	started	1	Feb 07 12:54:41 PM PST	13772	3728	0
3.	<input type="checkbox"/>	dispatcher	started	1	Feb 07 12:54:42 PM PST	13773	3746	0
4.	<input type="checkbox"/>	lockmanager	started	1	Feb 07 12:54:41 PM PST	13771	3733	0
5.	<input type="checkbox"/>	nspoller	started	1	Feb 07 12:54:36 PM PST	0	3761	0
6.	<input type="checkbox"/>	scheduler	started	1	Feb 07 12:57:07 PM PST	13798	3721	0
7.	<input type="checkbox"/>	httpd	started	2	Feb 07 12:58:55 PM PST	13807	3752	0
8.	<input type="checkbox"/>	dbpoller	started	1	Feb 07 12:54:36 PM PST	0	3766	0
9.	<input type="checkbox"/>	cnsserver	started	1	Feb 07 12:54:42 PM PST	13777	3763	0

- Step 4** On the ISC server, use the **wdclient status** command to find out the detailed status of the server.

**Symptom 2**

The service request is in the Wait Deployed state.

**Recommended Action**

This concerns the devices that are configured to use the CNS 2100 Series Intelligence Engine as the access method. If the devices are offline and a configlet was generated for it, the service request will move into the Wait Deployed state. As soon as the devices come online, the list of configlets will be downloaded and the status of the device will change.

**Symptom 3**

The service request is in the Failed Audit state.

**Recommended Action**

At least one command is missing on the device.

- 
- Step 1** From the ISC user interface, go to **Service Request Editor > Audit > Audit Config**.
- Step 2** Check the list of commands that are missing for each device.
- Step 3** Look for any missing command that has an attribute with a default value.
- 

**Symptom 4**

The service request is in the same state as it was before a deployment.

**Recommended Action**

If after a deployment a service request state remains in its previously nondeployed state (Request, Invalid, or Pending), it's an indication that the provisioning task did not complete successfully. Use the steps described in General Troubleshooting Guidelines, page C-2 to find out the reason for the service request failure.

**Symptom 5**

You receive the following out-of-memory error: *OutOfMemoryError*.

**Recommended Action**

- 
- Step 1** Open the Host Configuration dialog by choosing **Administration > Control Center**.  
The Control Center Hosts page is displayed.
- Step 2** Click the check box for the host of interest.  
The menu buttons for the Hosts page are enabled.
- Step 3** Click **Config**.  
The Host Configuration window is displayed.
- Step 4** Navigate to **watchdog > servers > worker > java > flags**.
- Step 5** Change the following attribute:  
Change the *Xmx256M* attribute to **Xmx384M** or **Xmx512M**.
- 

## Troubleshooting MPLS VPN and Layer 2 VPN

Go through the troubleshooting steps described in General Troubleshooting Guidelines, page C-2. If you have failed to troubleshoot or identify the problem, the information in this section provides information on how to gather logs for the development engineer to troubleshoot.

**Tip**


---

The logs apply to both MPLS VPNs and Layer 2 VPNs.

---

There is a property in DCPL called **Provisioning.Service.mpls.saveDebugData**. If this property is set to **True**, whenever a service request is deployed, a temporary directory is created in *ISC\_HOME/tmp/mpls*.

The directory contains the job ID of the service request prefixed to it, along with a time stamp. This directory contains the uploaded configuration files, service parameters in XML format, and the provisioning and audit results.

The default is set to True.

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | To verify, you can locate the property by choosing <b>Administration &gt; Control Center</b> .<br>The Control Center Hosts page is displayed. |
| <b>Step 2</b> | Click the check box for the host of interest.<br>The menu buttons for the Hosts page are enabled.   |
| <b>Step 3</b> | Click <b>Config</b> .<br>The Host Configuration window is displayed.  |
| <b>Step 4</b> | Navigate to <b>Provisioning &gt; mpls</b> .   |
| <b>Step 5</b> | Click <b>saveDebugData</b> .  |
- 

## Frequently Asked Questions

Below is a list of FAQs concerning MPLS VPN provisioning. (Question 13 pertains to Layer 2 VPNs.)

**Q 1:** Why does my service request go to Invalid when I select provisioning of an extra CE Loopback interface?

It is possible that the auto pick option of the IP addresses was selected for the service request, but a /32 IP address pool was not defined. Check and make sure the IP address and the IP address pool defined for this service request are compatible.

**Q 2:** When saving a service request, why does it say “CERC not initialized”?

It is necessary to pick a CERC for the link to join. Please check the service request to see if a CERC was selected.

**Q 3:** Why does creation of a VLAN ID pool require an Access Domain?

VLAN ID pools are associated with an Access Domain. Access Domains model a bridged domain; VLAN IDs should be unique across a Bridged Domain.

PE-POPs must be associated with an Access Domain. An Access Domain can have more than one PE-POP associated with it.

**Q 4:** In a Paging table, why are the **Edit** and **Delete** options disabled, even though only one check box is checked?

This is possible if one or more check boxes are selected in previous windows.

**Q 5:** Why can I not edit an MPLS VPN or L2VPN policy?

If a service request is associated with a policy, that policy can no longer be edited.

**Q 6:** I’m unable to create a CERC—can you explain why?

You have to define a Route Target pool before you create a CERC, unless you specify the Route Targets manually.

**Q 7:** How can I modify the configlet download order between the PE, CE, and PE-CLE devices?

There is a property called **Provisioning.Services.mpls.DownloadWeights.\*** that allows you to specify the download order for the following device types: PE, CE, PE-CLE, and MVRF CE.

For example, to ensure that the configlet is downloaded to the PE before it's downloaded to the CE, configure the **Provisioning.Services.mpls.DownloadWeights.weightForPE** property with a weight value greater than that of the CE.

**Q 8:** What does this property **Provisioning.Service.mpls.reapplyIpAddress** do?

If this property is set to True, during deployment of a decommissioned service request, this property will keep the IP address on the CE and PE intact on the router to maintain IPv4 connectivity to the CE.

**Q 9:** When I create a multi-hop NPC between a CE and PE through at least one PE-CLE device, why do I see some extra NPCs created?

IP Solution Center creates the extra NPCs to prevent operators from having to enter the same information again. A CE can now be connected to the PE-CLE device, and a new NPC will be created that will connect the new CE to a PE over the PE-CLE-to-PE NPC link.

**Q 10:** During service request provisioning, in the Interface selection list box, why don't I see the entire list of interfaces on the device?

This is probably due to a particular interface type being specified in the service policy. If that is the case, only interfaces of the specified interface type are displayed.

**Q 11:** Why do BGP and EIGRP not appear in the Routing protocol selection list for a service request associated to a No-CE policy?

BGP and EIGRP require certain CE-related parameters, such as the customer AS number and the CE's IP address. Since none of these parameters are requested in a No-CE policy, it is not feasible to provision these protocols. To provision a service request with BGP or EIGRP, use a policy with the **CE present** option specified, and you can set the CE to **unmanaged**.

**Q 12:** Why do the routing protocols BGP and EIGRP not appear when I select **No CE**?

If there is no CE in the scenario, BGP and EIGRP are not supported.

**Q 13:** This is a Layer 2 VPN question: Why does my service request go to Invalid with the message "loopback address missing"?

This is because the loopback address required to peer the pseudowire between PEs has not been defined in the PE-POP object in ISC.

## Troubleshooting IPsec Mapping into MPLS

IPsec mapping into MPLS consists of an IPsec service request and an MPLS service request. Each has its own debugging mechanism. There is no common debugging methodology for both IPsec and MPLS since they are two independent service requests. - **IPsec is not supported in this release.** -



## A

---

- about IP addresses in Cisco ISC 5-7
- access domain A-14
- Access Domain Management 12-11
- accessing MPLS reports 14-1
- Access Port 12-11
- ACLs
  - on the PE-CE link A-31
  - role in MPLS security A-30
- adding
  - CLE service request 6-33
  - PE-CE Links to the Management VPN 9-16
- adding a new customer CPE 2-5
- adding a new provider PE 2-12
- address space and routing separation A-27
- address space separation A-27
- advertised routes 6-16
- allowas-in option 5-23
- API
  - approach A-11
  - functionality supported A-11
- assigning IP address
  - automatically 5-13
- attacks, types of A-29
- audience, for guide xi
- auditing service requests 6-37
- autonomous system (AS) number
  - number of occurrences in as path 5-23
- autonomous systems, spanning 13-1
- auto-pick route target values 4-7

## B

---

- backbone carrier
  - definition 11-1
- backbone network
  - with a customer carrier ISP 11-1
  - with customer carrier BGP/MPLS VPN service provider 11-3
- benefits of cable MPLS VPNs 10-1
- BGP 5-21, A-13
  - allowas-in option 5-23
  - as number for CE's network 5-22
  - community attribute A-33
  - dampening A-30
  - neighbor allowas-in value 5-22
  - neighbor AS-override option 5-23
  - RDs and RTs A-24
  - redistribute connected routes 5-22
  - redistributing protocols into BGP 5-23
  - route-target communities A-25
  - security features A-33
- BGP protocol chosen 5-21
- Border Gateway Protocol. See BGP
- broken state 6-2
- business application A-1

## C

---

- cable MPLS VPN network 10-2
- cable services
  - cable-CE, creating 10-6
  - CMTS 10-4
  - DOCSIS 10-4
  - maintenance subinterface, provisioning 10-6

- MSO **10-4**
  - primary IP address range **10-5**
  - redistributing connected routes recommended **5-33**
  - redistributing static routes **5-33**
  - secondary IP address range **10-5**
  - specifying no routing protocol **5-33**
- cable VPN
  - configuration overview **10-4**
  - interfaces and subinterfaces **10-5**
- carrier supporting
  - carrier overview **11-1**
- carrier supporting carrier. See CSC.
- CE
  - BGP as number for **5-22**
  - cable-CE, creating **10-6**
  - default routes to **5-15**
  - description of **A-12**
  - extra loopback address **5-13**
  - managed CE considerations **9-2**
  - and MCE **9-4, 9-7**
  - OSPF process ID **5-25**
  - routing context table **A-32**
  - unmanaged CEs **9-1**
- CE interface information **5-12**
- CE present **5-8**
- CERC **5-40**
  - auto-pick route target values **4-7**
  - creating **4-6**
  - full mesh **A-26**
  - overview **A-25**
  - route target values, entering **4-7**
- CERC not initialized **C-5**
- CE Routing Communities **A-25**
- closed state **6-2**
- CMTS **10-4**
- CNS 2100 Series Intelligence Engine
  - wait deployed state **C-3**
- collect
  - configuration **2-8**
- collection server **A-4, A-12**
- common provisioning issues **C-2**
- confederation **13-8**
- configuration audit **6-38**
  - how to perform **6-38**
  - where to find **6-38**
  - why it could fail **6-39**
- configuration files
  - editing **6-39**
  - security requirement **A-32**
  - viewing **6-39**
- Configuring ETTH **12-11**
- Configuring NPC Ring Topology **12-4**
- connected routes, redistributing **5-21, 5-24, 5-28, 5-32**
- connectivity between VPNs **A-32**
- creating
  - access domain **2-15, 2-17**
  - cable link service request **10-11**
  - cable subinterface service request **10-6**
  - ce routing communities **4-6**
  - CPE **2-11**
  - customer **2-10**
  - customer, site, and cpe **2-10**
  - device **2-6**
  - device group **2-14**
  - IP address pool **3-2**
  - IP multicast VPN **4-3**
  - MCE Service Request **9-9**
  - MPLS service policy for PE-to-CE link **5-7**
  - MPLS VPN **4-1**
  - MPLS VPN in ISC **5-1**
  - MPLS VPN MVRFCE PE-CE Service Policies **8-6**
  - MPLS VPN MVRFCE PE-CE Service Requests **8-18**
  - MPLS VPN PE-CE Service Policies **7-5**
  - MPLS VPN PE-CE Service Requests **7-14**
  - multicast pool **3-4**
  - multi-VRF service request **6-17**
  - MVRFCE PE-CE Service Policy **8-6**
  - MVRFCE PE-CE Service Request **8-18**

- MVRFCE PE-CE service request **6-17**
- MVRFCE PE-NoCE Service Request **8-27**
- PE-CE Service Policy **7-6**
- PE-CE Service Request **7-14**
- PE-CE service request **6-6**
- PE-NoCE Service Policy **7-10, 8-12**
- PE-NoCE Service Request **7-21**
- PE-only service request **6-26**
- provider and a PE **2-14**
- region for the PE **2-14**
- route distinguisher pool **3-6**
- route target pool **3-7**
- service policies **5-6**
- service requests **6-5, 10-6**
- site **2-10**
- site of origin pool **3-9**
- VC ID pool **3-11**
- VLAN pool **3-13**
- Creating a Ring of Three PE-CLE **12-2**
- creating custom reports **14-6**
- CSC
  - creating service request **11-5**
  - defining a service policy **5-15, 5-16, 5-18, 5-22, 5-25, 5-29, 5-33**
  - defining service policy **11-5**
  - definition **11-1**
  - using MPLS **11-2**
- CSC support **5-15**
- customer carrier
  - as BGP/MPLS service provider **11-3**
  - definition **11-1**
- customer view **A-16**

## D

- dampening **A-30**
- Data Over Cable Service Interface Specifications. See DOCSIS
- default information originate option **5-17**

- default routes **5-18**
- default routes to CE **5-15**
- defining
  - CE as an MCE **9-8**
  - CSC service policy **11-5**
  - MVRFCE PE-CE service policy **5-34**
- Defining a VPN for the MVRFCE PE-CE Link **8-4**
- Defining a VPN for the PE-CE Link **7-3**
- defining the service policy VRF and VPN information **5-39**
- denial-of-service attack **A-29**
- deployed state **6-2**
- deploying service requests **6-33**
- device access algorithm **6-4**
- Device Configuration Service (DCS) **C-1**
- DOCSIS **10-4**
- documentation **xiii**
- document organization **xi**
- download order for devices, specifying **C-6**

## E

- EBGP **5-21**
- edge device routers
  - access algorithm **6-4**
- editable attributes **5-6**
- editing
  - configuration files **6-39**
  - PE with ISC GUI **2-15**
- EIGRP **5-28**
  - metrics **5-30**
  - protocol chosen **5-28**
- encapsulations for each interface type **5-10**
- ensuring VPN isolation **A-34**
- Ethernet-To-The-Home **12-9**
- ETTH Overview **12-9**
- exchanging VPN routing information **13-4**
- export route map
  - defining name of **5-39**

extra CE loopback required **5-13**  
 extranets **A-22**

## F

failed audit state **6-3, C-3**  
 failed deploy state **6-3**  
 frame relay  
   IETF encapsulation **5-11**  
 frequently asked questions **C-5**  
 full mesh considerations **A-26**  
 full mesh topology **A-26**  
   definition **A-25**  
 functional audit **6-37**  
   how to perform **6-37**  
   where to find **6-37**  
   why it could fail **6-38**  
 functional state **6-3**

## G

gateway of last resort **5-18**  
 general troubleshooting guidelines **C-2**  
 Generic Transport Library (GTL) **C-1**  
 getting started **1-1**  
   creating CERCs **1-3**  
   creating customer sites **1-2**  
   creating PEs **1-2**  
   creating provider **1-2**  
   creating region **1-2**  
   creating VPNs **1-3**  
   customer information **1-2**  
   devices **1-2**  
   license **1-1**  
   populating ISC **1-1**  
   provider information **1-2**  
   resource information **1-3**  
   resource pools **1-3**  
   route distinguisher pool **1-3**

route target pool **1-3**  
 giving only default routes to CE **5-15**

## H

hiding MPLS core structure **A-28**  
 hub and spoke considerations **A-26**  
 hub-and-spoke topology **A-26**  
   definition **A-25**  
 hub route target **5-5**

## I

IBGP **5-21**  
 IGMP with MVR **12-11**  
 IGP route label **13-6**  
 implementation techniques **9-4**  
 import route map  
   defining name of **5-39**  
 in-band connection **9-4**  
 Infrastructure Data **7-3, 8-3**  
 inter-autonomous systems  
   benefits **13-2**  
   confederation **13-8**  
   IGP route label **13-6**  
   neighbor next-hop-self command **13-3**  
   overview **13-1**  
   redistribute connected command **13-5**  
   redistribute connected subnets command **13-4**  
   routing between AS's' **13-2**  
   VPN route label **13-6**  
 interfaces  
   cable maintenance subinterface, provisioning **10-6**  
   encapsulations available **5-10**  
   IP numbered **5-13**  
   loopback, using existing number **5-14**  
   subinterface numbers, how chosen by VPNSC **10-5**  
   supported interfaces **5-9**  
 Internet Service Provider. See ISP

intranets **A-22**  
 Intranets and Extranets **A-22**  
 intrusion attack **A-29**  
 invalid state **6-3**  
 inventory and connection manager **5-2**  
 IP address  
     keeping IP addresses on CE and PE intact **C-6**  
 IP addresses **5-7**  
     automatically assigned **5-13**  
     IP numbered with extra CE loopback **5-13**  
     and network security **A-34**  
     numbered **5-13**  
     primary IP address range **10-5**  
     secondary IP address range **10-5**  
     unnumbered **5-13**  
     VPN-IPv4 address **5-40**  
     VPN-IPv4 address **A-27**  
     in VPNs **A-13**  
 IP address pool **5-13**  
 IP address pool, create a **3-2**  
 IP address pools  
     and automatically assigned addresses **5-13**  
     and regions **5-13**  
     on the PE-CE link **5-7**  
 IP numbering scheme **5-12**  
 IP Solution Center  
     collection server **A-12**  
     network management subnet **A-12**  
     processing server **A-12**  
     servers, status of **C-3**  
 ip solution center  
     device access algorithm **6-4**  
 IP Solution Center Overview **A-1**  
 IPv4 BGP label distribution **11-4**  
 ISC configuration options **11-4**  
 ISC ETTH Implementation **12-11**  
 ISP **10-5**  
     secondary IP address range **10-5**  
 issues regarding access to VPNs **9-4**

## L

label spoofing **A-30, A-31**  
 LDP/IGP **11-4**  
 LDP Authentication **A-32**  
 LDP authentication **A-32**  
 load balancing **A-5**  
 loopback  
     extra loopback address on CE **5-13**  
     interface number, using existing **5-14**  
     and ip unnumbered addressing scheme **5-13**  
     SR ID not included **5-14**  
 loopback address missing **C-6**  
 lost state **6-3**

## M

managed CE  
     considerations **9-2**  
 Managed Customer Edge Routers **9-2**  
 Management CE (MCE) **9-4**  
 Management CE. See MCE  
 Management PE (MPE) **9-5**  
 Management PE. See MPE  
 management route map **9-6**  
 Management VPN **9-5**  
 management VPN **9-5, A-12**  
     and export route map **5-39**  
     in cable network **10-4**  
     and management route map **9-6**  
     PE-CE links, provisioning **9-16**  
     redistribute connected routes required **5-17**  
     topology **9-5**  
 maximum number of routes into VRF **5-40**  
 MCE **9-4, 9-7**  
 monitoring  
     task logs **2-10**  
 monitoring service requests **6-35**  
 MP-BGP Security Features **A-33**

- MPE 9-5
  - and shadow CE 9-5
- MPLS PE service report 14-3
  - filter values 14-3
  - output values 14-3
- MPLS reports
  - accessing 14-1
  - creating custom 14-6
  - overview 14-1
  - running 14-4
- MPLS Service Activation 1-1
- MPLS service activation 1-1
- MPLS service request report 14-5
  - filter values 14-5
  - output filters 14-5
- MPLS services
  - provisioning workflow C-1
- MPLS VPN A-20
- MPLS VPN MVRFCE PE-CE Link Overview 8-1
- MPLS VPN PE-CE Link Overview 7-1
- MPLS VPN Provisioning Workflow C-1
- MPLS VPNS
  - routing protocols 5-15
- MPLS VPNs A-20
  - address space separation A-27
  - CERCs in A-25
  - characteristics A-21
  - connectivity between A-32
  - default routes to CE 5-15
  - extranets A-22
  - implementation techniques 9-4
  - in-band connection 9-4
  - intranets A-22
  - management VPN 9-5
  - multiple VPNS merged into a single VPN A-33
  - out-of-band VPN 9-5
  - principal technologies A-21
  - route-target communities A-25
  - routing separation A-27
  - service requests, defining 6-26, 9-9, 10-6, 10-11
  - VRF forwarding table A-32
- MPLS VPN Security A-27
- MPLS VPN Solution
  - security requirements A-27
- MPLS VPN topology example 6-5
- MSO
  - domain 10-4
  - primary IP address range 10-5
- multicast
  - data MDT size 5-4
  - data MDT threshold 5-4
  - enabling 5-4
  - multicast domain (MD) 5-4, 6-4
  - multicast VRF 5-4, 6-4
- multicast pool, create a 3-4
- multiple VPNS merged into a single VPN A-33
- Multi-VPN routing and forwarding tables 2-1
- multi-VRF
  - example 6-5
  - overview 6-17
- Multi-VRF CE A-18
  - data path A-19
  - description of A-18
  - switch supported for A-18
  - unlike a CE A-19
- MVRF 2-1
- MVRFCE CE Information 8-32
- MVRFCE PE-CE
  - policy type 2-4
- MVRFCE PE-CE Link
  - creating a Service Policy 8-6
  - creating a Service Request 8-18
  - defining a VPN 8-4
  - overview 8-1
- MVRFCE PE-CE link
  - creating a service policy 5-34
- MVRFCE PE-NoCE Link
  - creating a Service Policy 8-12

creating a Service Request **8-27**

## N

NBI Benefits **A-11**

neighbor allowas-in value **5-22**

neighbor AS-override option **5-23**

neighbor next-hop-self command **13-3**

network devices

how ISC accesses **6-4**

network inventory **2-2**

network layer reachability information. See NLRI

network management subnet **A-12**

management VPN technique **9-5**

out-of-band technique **9-7**

Network Management Subnets **9-3**

Network Topology **7-2, 8-2**

NLRI **A-21**

none chosen

cable services **5-33**

North Bound Interface (NBI) **A-10**

NPC

Ring Topology **12-2**

NPC Ring Topology **12-1**

## O

OSPF **5-24**

area number on PE **5-26**

connected routes, redistributing **5-25**

process ID on CE **5-25**

process ID on PE **5-25**

OSPF protocol chosen **5-24**

Out-of-Band Technique **9-7**

out-of-band technique **9-5, 9-7**

out-of-memory error **C-4**

overview

access domain **2-16**

ISC customer **2-5**

ISC management network **9-1**

ISC provider **2-13**

of MPLS VPN cable **10-1**

resource pools **3-1**

overview of service requests **6-1**

## P

PE

description of **A-18**

export route map **5-39**

import route map **5-39**

and MPE **9-5**

OSPF area number **5-26**

OSPF process ID **5-25**

PE-CE

example **6-5**

PE-CE Interface **A-31**

PE-CE Link

creating a Service Policy **7-5**

creating a Service Request **7-14**

defining a VPN **7-3**

PE-CE link

for management VPN **9-16**

routing protocols for **5-15**

security considerations **A-31**

static route for IP unnumbered scheme **5-13**

static route provisioning **5-16**

PE-CE Service Policy Overview **7-5**

PE-CLE

Ring Topology **12-2**

PE Information **7-18, 8-31**

pe interface information **5-9**

pending state **6-3**

PE-NoCE Link

creating a Service Policy **7-10**

creating a Service Request **7-21**

PE-only

example **6-5**

- point-to-point address pool **5-13**
- policy
  - name **5-8**
  - owner **5-8**
- Policy for Residential Services Over Shared VLAN **12-16**
- pos interface **5-11**
- Prerequisite Tasks **7-2, 8-3**
- primary IP address range **10-5**
- processing server **A-4, A-12**
- process overview **2-2**
- provider edge routers **A-18**
- Provider View **A-17**
- provisioning
  - cable maintenance subinterface **10-6**
- Provisioning.Service.mpls.saveDebugData property **C-5**
- provisioning a CSC service request **11-5**
- provisioning a management CE in ISC **9-7**
- provisioning cable services in ISC **10-6**
- Provisioning driver (ProvDrv) **C-1**
- PVLAN or Protected Port **12-11**

## R

- RD
  - allocate new RD **5-40**
  - description of **A-24**
  - in hub-and-spoke environments **A-26**
  - overwriting default RD value **5-40**
  - role in routing separation **A-27**
- redistribute connected **5-21, 5-24, 5-28, 5-32**
- redistribute connected command **13-5**
- redistribute connected subnets command **13-4**
- redistribution of IP routes **5-15**
- redistribution of routing information **5-19**
- regions
  - ip address pools **5-13**
- related documentation **xiii**
- reports **14-1**
- requested state **6-3**
- Residential Service **12-15**
- resistance to attacks **A-28**
- resource pools **1-3, 3-1, A-15**
- Ring Topology **12-1**
  - configuring Ring Topology **12-4**
  - NPC **12-2**
  - PE-CLE **12-2**
- Ring Topology Overview **12-1**
- RIP
  - default route to CE **5-18**
  - giving only default routes to CE **5-18**
  - hop counts **5-19**
  - metrics **5-19**
  - redistributing connected routes **5-18**
  - redistributing OSPF routes to a PE **5-21, 5-24, 5-28**
  - redistributing static routes **5-18**
  - route provisioning **5-18**
- RIP protocol chosen **5-17**
- Role-Based Access Control (RBAC) **A-10**
- route distinguisher **5-40**
- route distinguisher. See RD
- route distinguisher pool **1-3**
- route distinguisher pool, create a **3-6**
- route distinguishers and route targets **A-24**
- route map
  - export **5-39**
  - import **5-39**
- routers
  - access algorithm **6-4**
  - redistribute connected **5-21, 5-24, 5-28, 5-32**
  - redistribution **5-19**
  - routing context table **A-32**
  - VRF forwarding table **A-32**
- routes to reach other sites **6-16**
- route target. See RT
- route target communities **A-25**
- route-target communities **A-25**
- route target pool **1-3**
- route target pool, create a **3-7**

- routing
    - authentication **A-32**
    - separation **A-27**
  - routing between autonomous systems **13-2**
  - routing between subautonomous systems in a confederation **13-8**
  - routing context table **A-32**
  - routing protocols
    - defining for PE-CE link **5-15**
    - redistribute connected **5-21, 5-24, 5-28, 5-32**
    - redistribution **5-19**
    - securing **A-29**
  - routing separation **A-27**
  - RT
    - description of **A-24**
    - entering RT values in CERC definition **4-7**
- ## S
- 
- secondary IP address range **10-5**
  - securing
    - MPLS core **A-31**
    - routing protocol **A-29**
  - security considerations
    - address space and routing separation **A-27**
    - connectivity between VPNs **A-32**
    - denial-of-service attack **A-29**
    - hiding the MPLS core structure **A-28**
    - intrusion attack **A-29**
    - label spoofing **A-31**
    - PE-CE link **A-31**
  - security requirements for MPLS VPNs **A-27**
  - security through IP address resolution **A-34**
  - separation of CE-PE Links **A-32**
  - servers
    - status of **C-3**
    - wdclient status command **C-3**
  - multi-VRF CE
    - in service provider network **A-12**
  - service audit **A-19**
  - service enhancements **6-4**
  - service module **C-2**
  - service operator **5-6**
  - service policy **2-4, 5-6**
    - CERC membership **5-40**
    - editable attributes **5-6**
    - editor **5-6**
    - entering values **5-6**
    - interface attributes **5-8**
    - overview **5-1**
    - VRF and VPN information **5-39**
  - service provider network **A-12**
  - service request **2-4**
    - states **6-2**
    - transition states **6-1**
  - service requests **12-17**
    - defining **6-26, 9-9, 10-6, 10-11**
    - deploying **6-33**
    - RD value, overwriting **5-40**
    - service policy **5-6**
    - templates, enabling **5-40**
    - VRF name, overwriting **5-40**
  - shadow CE
    - and Management PE **9-5**
  - site of origin **6-4**
  - site of origin pool, create a **3-9**
  - specifying
    - IP address scheme **5-12**
    - PE and CE interface parameters **5-8**
    - routing protocol for a service **5-15**
  - spoke route target **5-5**
  - state
    - broken **6-2**
    - closed **6-2**
    - deployed **6-2**
    - failed audit **6-3**
    - failed deploy **6-3**
    - functional **6-3**

- invalid **6-3**
- lost **6-3**
- pending **6-3**
- requested **6-3**
- wait deployed **6-3**
- states of service requests **6-2**
- static protocol chosen **5-16**
- static route provisioning **5-16**
  - created for IP unnumbered link **5-13**
  - default information originate option **5-17**
  - giving default routes to CE **5-16**
  - redistributing connected routes **5-17, 5-22, 5-29, 5-32, 5-33**
- static routing protocols **6-14**
- subinterface numbers, how chosen by VPNSC **10-5**
- system
  - architecture **A-2**
  - features **A-7**

## T

- task does not execute **C-3**
- template manager **A-9**
- templates
  - enabling for service policy **5-40**
- terms defined **C-2**
- troubleshooting
  - IPsec Mapping into MPLS **C-6**
  - MPLS VPN and Layer 2 VPN **C-4**
- trusted devices **A-31**

## U

- UNI security information **5-11**
- unmanaged CEs **9-1**
- unmanaged customer edge routers **9-1**
- unmanaged MVRFC
  - overview **2-1**
  - select management type **2-12**
- unnumbered IP addresses **5-13**

- using existing loopback interface number **5-14**
- using ISC to span multiple autonomous systems **13-10**

## V

- vc id pool, create a **3-11**
- VLAN
  - ID, automatically set by ISC **5-11**
- VLAN ID pool and access domain **C-5**
- vlan pool, create a **3-13**
- VPN
  - auto-pick route target values **4-7**
  - route label **13-6**
- VPN-IPV4 address **5-40**
- VPN-IPv4 address **13-11, A-27**
- VPN Profile **A-16**
- VPN route forwarding table. See VRF
- VPN route label **13-6**
- VPN Routing and Forwarding Tables **A-22**
- VPNs
  - creating **5-1**
  - issues regarding access to **9-4**
  - multicast routing **5-4**
- VRF **A-21**
  - configuration commands **A-24**
  - Description **5-40**
  - elements of **A-22**
  - export route map, defining name of **5-39**
  - implementation **A-23**
  - implementation considerations **A-23**
  - import route map, defining name of **5-39**
  - instance **A-24**
  - maximum routes in **5-40**
  - multicast VRF **5-4, 6-4**
  - naming convention **A-22**
  - overwriting VRF name **5-40**
  - and route-target communities **A-25**
  - and routing separation **A-27**
  - subinterface associated with **10-5**

VRF forwarding table **A-32**

## W

wait deployed state **6-3, C-3**

wan interfaces

    loopback, using existing loopback number **5-14**

wdclient command **C-3**

