



Cisco IP Solution Center MPLS VPN User Guide, 5.1

Americas 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: 408 527-0883

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

MPLS User Guide, 5.1

© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

About This Guide	xiii
Objective	xiii
Audience	xiii
Organization	xiii
Related Documentation	xiv
Obtaining Documentation and Submitting a Service Request	xv

CHAPTER 1

Getting Started with MPLS VPN	1-1
Before You Begin	1-1
ISC Service Activation	1-1
Working with MPLS Policies and Service Requests	1-2

CHAPTER 2

Setting Up the ISC Services	2-1
Overview	2-1
Creating Devices	2-2
Creating Logical Devices	2-3
Collecting Configurations	2-4
Monitoring Task Logs	2-5
Creating Device Groups	2-6
Setting Up Devices for IOS XR Support	2-6
Creating Customers, Sites, and CPEs	2-7
Creating Customers	2-8
Creating Sites	2-8
Creating CPEs	2-8
Creating Providers, Regions, and PEs	2-9
Creating a Provider	2-10
Creating a Region for PE	2-11
Creating PEs	2-11
Editing PEs	2-12
Creating Access Domains	2-12
Creating Resource Pools	2-15
Overview of Resource Pools	2-15
Creating an IPv4 Address Pool	2-16

Creating a Multicast Pool	2-16
Creating a Route Distinguisher Pool	2-17
Creating a Route Target Pool	2-18
Creating a Site of Origin Pool	2-19
Creating a VC ID Pool	2-20
Creating a VLAN Pool	2-21
Defining VPNs	2-22
Creating an MPLS VPN	2-22
Creating an IP Multicast VPN	2-26
Enabling a Unique Route Distinguisher for a VPN	2-28
Provisioning MPLS Service Requests Using Unique Route Distinguisher	2-29
Creating CE Routing Communities	2-32

CHAPTER 3

Independent VRF Management 3-1

Overview	3-1
Working with VRF Objects	3-2
Creating a New VRF Object	3-2
Copying a VRF Object	3-5
Searching for VRF Objects in the ISC Repository	3-7
Modifying Non-Deployed VRF Objects	3-7
Single-VRF Edit Mode	3-7
Multi-VRF Edit Mode	3-7
Modifying Deployed VRF Objects	3-9
Deleting VRF Objects	3-10
Deleting VRF Objects Associated with VRF Service Requests	3-10
Working with VRF Service Requests	3-11
Overview of VRF Service Requests	3-11
Defining VRF Service Requests	3-11
Deploying VRF Service Requests	3-13
Modifying VRF Service Requests	3-14
Decommissioning and Deleting VRF Service Requests	3-14
Searching for VRF Service Requests by VRF Object Name	3-15
Viewing the Configlet Generated by a Deployed VRF Service Request	3-15
Using VRFs with MPLS VPN Service Requests and Policies	3-16
Relationship of VRF Object and Service Requests and PE Device	3-16
Specifying VRF Objects within MPLS VPN Service Requests	3-16
Notes On Using a VRF Object in an MPLS Service Request	3-20
Searching for MPLS VPN Service Requests by VRF Object Name	3-20
Specifying VRF Objects within MPLS VPN Service Policies	3-20

Migrating Existing MPLS VPN Service Requests to the VRF Object Model 3-21

CHAPTER 4

IPv6 and 6VPE Support in MPLS VPN 4-1

Overview of IPv6 and 6VPE 4-1

Internet Protocol Version 6 (IPv6) 4-1

IPv6 VPN Provider Edge Router (6VPE) 4-2

Comparison of IOS and IOS XR 4-3

General Comparison of IOS and IOS XR Device Configlets 4-3

VRF-Related Configlets 4-4

Interface-Related Configlets 4-4

Using OSPF as the PE-CE Routing Protocol 4-4

Using EIGRP as the PE-CE Routing Protocol 4-5

Using Static as the PE-CE Routing Protocol 4-5

Multicast Routing on IOS XR Devices 4-6

ISC and MPLS VPN Updates to Support IPv6 and 6VPE 4-7

Inventory and Device Management 4-7

VPN Creation and Configuration 4-8

VRF Object Support 4-8

Resource Pools 4-9

MPLS VPN Service Provisioning 4-9

MPLS VPN Service Policies 4-9

MPLS VPN Service Requests 4-10

MPLS Service Request Audits 4-11

MPLS Reports 4-11

IPv6 and 6VPE Features Not Supported in ISC 5.1 4-11

CHAPTER 5

MPLS VPN Service Policies 5-1

Service Policy Overview 5-1

Service Policy Editor 5-1

About IP Addresses in Cisco ISC 5-2

Defining an MPLS VPN Service Policy 5-2

Specifying PE and CE Interface Parameters 5-4

Specifying the IP Address Scheme 5-8

Using Existing Loopback Interface Number 5-10

Specifying the Routing Protocol for a Service 5-11

Redistribution of IP Routes 5-12

CSC Support 5-12

Giving Only Default Routes to CE 5-12

Static Protocol Chosen	5-12
RIP Protocol Chosen	5-14
BGP Protocol Chosen	5-18
OSPF Protocol Chosen	5-21
EIGRP Protocol Chosen	5-24
None Chosen: Cable Services	5-28
Defining VRF and VPN Information	5-29
BGP Multipath Load Sharing and Maximum Path Configuration	5-32
Removing a Multipath Configuration	5-34
Enabling Template Association for a Policy	5-34

CHAPTER 6

MPLS VPN Service Requests 6-1

Overview of Service Requests	6-1
Service Request Transition States	6-1
Service Enhancements	6-5
How ISC Accesses Network Devices	6-5
Examples of Creating MPLS VPN Service Requests	6-6
MPLS VPN Topology Example	6-6
Creating an MPLS VPN PE-CE Service Request	6-7
Viewing Configlets Generated by the MPLS VPN Service Request	6-13
Setting Static Routing Protocol Attributes (for IPv4 and IPv6)	6-13
Creating a Multi-VRF Service Request	6-15
Creating a PE-Only Service Request	6-20
Adding a CLE to a Service Request	6-25
Deploying Service Requests	6-25
Monitoring Service Requests	6-27
Auditing Service Requests	6-28
Functional Audit	6-28
How to Perform a Functional Audit	6-28
Where to Find Functional Audit	6-29
Why Functional Audit Could Fail	6-29
Configuration Audit	6-29
How to Perform a Configuration Audit	6-30
Where to Find Configuration Audit	6-30
Why Configuration Audit Could Fail	6-30
Viewing Configlets Generated by a Service Request	6-31
Viewing Configlets on IOS XR Devices	6-32
Editing Configuration Files	6-33

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

Defining a VPN for the PE-CE Link 7-3

Creating MPLS VPN PE-CE Service Policies 7-3

PE-CE Service Policy Overview 7-3

Creating a PE-CE Service Policy 7-4

Creating a PE-NoCE Service Policy 7-6

Creating MPLS VPN PE-CE Service Requests 7-8

Creating PE-CE Service Requests 7-8

Creating PE-NoCE Service Requests 7-12

CHAPTER 8**Provisioning Multi-VRFCE PE-CE Links 8-1**

MPLS VPN MVRFCE PE-CE Link Overview 8-1

Network Topology 8-2

Prerequisite Tasks 8-3

Defining VPN for MVRFCE PE-CE Links 8-3

Creating MPLS VPN MVRFCE PE-CE Service Policies 8-4

Creating MVRFCE PE-CE Service Policies 8-4

Creating PE-NoCE Service Policies 8-6

Creating MPLS VPN MVRFCE PE-CE Service Requests 8-8

Creating MVRFCE PE-CE Service Requests 8-8

Creating MVRFCE PE-NoCE Service Requests 8-14

Creating an Unmanaged MVRFCE 8-19

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) 9-5

Management PE (MPE) 9-5

Management VPN 9-5

Advantages 9-6

Out-of-Band Technique 9-7

Provisioning a Management CE in ISC	9-8
Defining CE as MCE	9-8
Creating MCE Service Requests	9-10
Adding PE-CE Links to Management VPNs	9-14

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	10-3
Cable VPN Configuration Overview	10-4
Cable VPN Interfaces and Subinterfaces	10-5
Provisioning Cable Services in ISC	10-5
Creating the Service Requests	10-6
Creating a Cable Subinterface Service Request	10-6
Creating Cable Link Service Requests	10-10

CHAPTER 11

Provisioning Carrier Supporting Carrier 11-1

Carrier Supporting Carrier Overview	11-1
Backbone Network with ISP Customer Carrier	11-1
Backbone Network with BGP/MPLS VPN Service Provider Customer Carrier	11-3
ISC Configuration Options	11-4
LDP/IGP	11-4
IPv4 BGP Label Distribution	11-4
Defining CSC Service Policies	11-5
Provisioning CSC Service Requests	11-5

CHAPTER 12

Provisioning Multiple Devices 12-1

NPC Ring Topology	12-1
Ring Topology Overview	12-1
Creating Ring of Three PE-CLEs	12-2
Configuring NPC Ring Topology	12-5
Ethernet-To-The-Home (ETTH)	12-9
Access Domain Management	12-11
ISC ETTH Implementation	12-11
Creating an ETTH Policy	12-12
Creating a Service Request for ETTH	12-13

Residential Service 12-15

Creating a Policy for Residential Services Over Shared VLAN 12-16

Creating a Service Request for Residential Services Over Shared VLAN 12-18

CHAPTER 13**Spanning Multiple Autonomous Systems 13-1**

Overview 13-1

Benefits 13-2

Routing Between Autonomous Systems 13-3

Exchanging VPN Routing Information 13-4

Routing Between Subautonomous Systems in a Confederation 13-8

Using ISC to Span Multiple Autonomous Systems 13-9

Using Templates to Support Inter-Autonomous System Solutions 13-11

Inter-AS 10B Hybrid Model 13-11

Inter-AS RT-Rewrite 13-12

Creating the Inter-AS Templates 13-12

CHAPTER 14**Generating MPLS Reports 14-1**

Overview 14-1

Accessing MPLS Reports 14-1

Running Reports 14-2

MPLS PE Service Report 14-3

MPLS Service Request Report 14-4

MPLS Service Request Report - 6VPE 14-5

6VPE Supported Devices Report 14-6

Creating Custom Reports 14-7

APPENDIX A**Sample Configlets A-1**

Overview A-1

APPENDIX B**Working with Templates and Data Files B-1**

Overview B-1

Summary of Template Manager Features B-1

Template and Data File Workflow B-3

Using Templates with ISC Policies B-4

Overview of Template Support in ISC Policies B-4

Associating Templates and Data Files to a Policy B-4

Using Templates with Service Requests B-8

Overview of Template Use in Service Requests	B-8
Associating Templates to a Service Request	B-9
Associating Subtemplates During Service Provisioning	B-9
Creating Data Files During Service Request Creation	B-10
Using Negate Templates to Decommission Template Configurations	B-11
Using Templates and Data Files with Service Requests	B-12
Choosing a Template in the Service Request Workflow	B-12
Creating a Data File in the Service Request Workflow	B-14
Decommissioning Service Requests with Added Templates	B-15
Viewing Templates from the Service Requests Window	B-16

APPENDIX C

Troubleshooting MPLS VPNs C-1

General Troubleshooting Guidelines	C-1
Gathering Logs for Development Engineering	C-1
Frequently Asked Questions	C-2

APPENDIX D

Service Request Transition States D-1

APPENDIX E

MPLS VPN Concepts E-1

MPLS VPNs	E-1
Intranets and Extranets	E-2
VPN Routing and Forwarding Tables	E-3
VRF Implementation	E-4
VRF Instance	E-5
Independent VRF Object Management	E-5
Route Distinguishers and Route Targets	E-5
Route Target Communities	E-6
CE Routing Communities	E-6
Hub and Spoke Considerations	E-7
Full Mesh Considerations	E-8
MPLS VPN Security	E-8
Address Space and Routing Separation	E-8
Address Space Separation	E-8
Routing Separation	E-9
Hiding the MPLS Core Structure	E-9
Resistance to Attacks	E-10
Securing the Routing Protocol	E-10
Label Spoofing	E-12

Securing the MPLS Core	E-12
Trusted Devices	E-12
PE-CE Interface	E-12
Routing Authentication	E-13
Separation of CE-PE Links	E-13
LDP Authentication	E-13
Connectivity Between VPNs	E-13
MP-BGP Security Features	E-14
Security Through IP Address Resolution	E-15
Ensuring VPN Isolation	E-15

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 concepts:

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

Organization

This guide contains the following chapters:

- [Chapter 1, “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).
- [Chapter 2, “Setting Up the ISC Services,”](#) describes how to set up ISC services needed for MPLS policies and service requests.
- [Chapter 3, “Independent VRF Management,”](#) describes how to create, deploy and manage VRF objects independent of MPLS VPN links and service requests.
- [Chapter 4, “IPv6 and 6VPE Support in MPLS VPN,”](#) describes MPLS VPN support for IPv6 and 6VPE for this release.
- [Chapter 5, “MPLS VPN Service Policies,”](#) describes the Policy Manager GUI and work flow for MPLS VPN.
- [Chapter 6, “MPLS VPN Service Requests,”](#) describes the Service Requests GUI and work flow for MPLS VPN.

- [Chapter 7, “Provisioning Regular PE-CE Links,”](#) describes an end-to-end scenario for creating a regular PE-CE link.
- [Chapter 8, “Provisioning Multi-VRFCE PE-CE Links,”](#) describes an end-to-end scenario for creating a Multi-VRFCE PE-CE link.
- [Chapter 9, “Provisioning Management VPN,”](#) describes how to provision a management VPN in ISC.
- [Chapter 10, “Provisioning Cable Services,”](#) describes how to provision MPLS VPN cable services.
- [Chapter 11, “Provisioning Carrier Supporting Carrier,”](#) describes how to provision Carrier Supporting Carrier.
- [Chapter 12, “Provisioning Multiple Devices,”](#) describes how to provision Ethernet to the home, hub and spoke, and ring topologies.
- [Chapter 13, “Spanning Multiple Autonomous Systems,”](#) describes the network configuration for spanning multiple autonomous systems.
- [Chapter 14, “Generating MPLS Reports,”](#) describes how to set up, run, and format MPLS reports.
- [Appendix A, “Sample Configlets,”](#) shows various configlets generated by this application.
- [Appendix B, “Working with Templates and Data Files,”](#) provides information about using templates and data files in ISC policies and service requests.
- [Appendix C, “Troubleshooting MPLS VPNs,”](#) describes how to troubleshoot MPLS VPN.
- [Appendix D, “Service Request Transition States,”](#) describes the ISC service request transition states.
- [Appendix E, “MPLS VPN Concepts,”](#) provides an overview of MPLS VPN concepts and security considerations.

Related Documentation

The entire documentation set for Cisco IP Solution Center, 5.1 can be accessed at:

http://www.cisco.com/en/US/products/sw/netmgmtsw/ps4748/tsd_products_support_series_home.html



Tip

To cut and paste a two-line URL into the address field of your browser, you must cut and paste each line separately to get the entire URL without a break.

The following documents comprise the ISC 5.1 documentation set.

General documentation (in suggested reading order)

- *Cisco IP Solution Center Getting Started and Documentation Guide, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/roadmap/docguide.html
- *Release Notes for Cisco IP Solution Center, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/release/notes/relnotes.html
- *Cisco IP Solution Center Installation Guide, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/installation/guide/installation.html

- *Cisco IP Solution Center Infrastructure Reference, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/infrastructure/reference/guide/infrastructure.html
- *Cisco IP Solution Center System Error Messages, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/system/messages/messages.html

Application and technology documentation (listed alphabetically)

- *Cisco IP Solution Center Carrier Ethernet and L2VPN User Guide, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/carrier_ethernet/user/guide/l2vpn51book.html
- *Cisco IP Solution Center MPLS VPN User Guide, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/mps_vpn/user/guide/mps51book.html
- *Cisco IP Solution Center Traffic Engineering Management User Guide, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/traffic_management/user/guide/tem.html
- *Cisco MPLS Diagnostics Expert 2.1.3 Failure Scenarios Guide on ISC 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/mps_failure_scenarios/user/guide/mdefs.html
- *Cisco MPLS Diagnostics Expert 2.1.3 User Guide on ISC 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/mps_diagnostics/user/guide/mdeuser.html

API Documentation

- *Cisco IP Solution Center API Programmer Guide, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/developer/guide/api-gd.html
- *Cisco IP Solution Center API Programmer Reference, 5.1.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.1/developer/reference/xmlapi.zip



Note

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

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). It contains the following sections:

- [Before You Begin](#), page 1-1
- [ISC Service Activation](#), page 1-1
- [Working with MPLS Policies and Service Requests](#), page 1-2



Note

The information in the chapter summarizes some of the key tasks required to get started using MPLS VPN. For additional information about setting up basic ISC services, see [Chapter 2, “Setting Up the ISC Services”](#) and the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

Before You Begin

Before you can use MPLS VPN to provision, perform the following steps.

Step 1 Install ISC. See the [Cisco IP Solution Center Installation Guide, 5.1](#).

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 the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

ISC 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. The major steps to achieve ISC service activation include setting up:

- Devices
- Provider information (providers, regions, and PEs)

- Customer information (customers, sites, and CPEs)
- Resource pools:
 - IP addresses
 - Route targets (RTs)
 - Route distinguishers (RDs)
 - Site of origin (SOO)
- Virtual Private Networks (VPNs)
- Customer edge (CE) routing communities (CERCs)
- Named Physical Circuits (NPCs)

**Note**

These steps are covered in more detail in [Chapter 2, “Setting Up the ISC Services.”](#)

Working with MPLS Policies and Service Requests

After you have set up providers, customers, devices, and resources in ISC, you are ready to create MPLS policies, provision service requests, and deploy the services. After the service requests are deployed you can monitor, audit and run reports on them. All of these tasks are covered in this guide. To accomplish these tasks, perform the following steps.

-
- Step 1** If necessary, review overview information about MPLS concepts.
See [Appendix E, “MPLS VPN Concepts”](#)
- Step 2** Set up an MPLS policy.
For basic information and key concepts, see [Chapter 5, “MPLS VPN Service Policies,”](#) as well as subsequent chapters in this guide.
- Step 3** Provision the MPLS service request.
See the appropriate chapter, depending on the type service request you want to provision:
- [Chapter 3, “Independent VRF Management.”](#)
 - [Chapter 6, “MPLS VPN Service Requests.”](#)
 - [Chapter 7, “Provisioning Regular PE-CE Links.”](#)
 - [Chapter 8, “Provisioning Multi-VRFCE PE-CE Links.”](#)
 - [Chapter 9, “Provisioning Management VPN.”](#)
 - [Chapter 10, “Provisioning Cable Services.”](#)
 - [Chapter 11, “Provisioning Carrier Supporting Carrier.”](#)
 - [Chapter 12, “Provisioning Multiple Devices.”](#)
 - [Chapter 13, “Spanning Multiple Autonomous Systems.”](#)
- Step 4** Deploy the MPLS service request.
See [Chapter 6, “MPLS VPN Service Requests.”](#)

Step 5 Check the status of deployed services.

You can use one or more of the following methods:

- Monitor service requests. See the section [Monitoring Service Requests](#), page 6-27.
- Audit service requests. See the section [Auditing Service Requests](#), page 6-28.
- Run MPLS reports. See [Chapter 14, “Generating MPLS Reports.”](#)

Step 6 Troubleshoot MPLS services.

See [Appendix C, “Troubleshooting MPLS VPNs.”](#)

For additional information on specific topics, see the following sections of this guide:

- For information about IPv6 and 6VPE support, see [Chapter 4, “IPv6 and 6VPE Support in MPLS VPN”](#).
- For sample configlets generated by ISC for MPLS services, see [Appendix A, “Sample Configlets.”](#)
- For information about using templates and data files in ISC policies and service requests, see [Appendix B, “Working with Templates and Data Files.”](#)



CHAPTER 2

Setting Up the ISC Services

This chapter contains the basic steps to set up the Cisco IP Solution Center (ISC) services to support MPLS VPN service policies and service requests. It contains the following sections:

- [Overview, page 2-1](#)
- [Creating Devices, page 2-2](#)
- [Creating Customers, Sites, and CPEs, page 2-7](#)
- [Creating Providers, Regions, and PEs, page 2-9](#)
- [Creating Access Domains, page 2-12](#)
- [Creating Resource Pools, page 2-15](#)
- [Defining VPNs, page 2-22](#)
- [Creating CE Routing Communities, page 2-32](#)



Note

This chapter presents high-level information on ISC services that are relevant to MPLS VPN. For more detailed information on setting up these and other basic ISC services, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). 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 the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

Overview

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)

- VPN

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

- CE Routing Communities (CERC is optional)

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 covers the following topics:

- [Creating Logical Devices, page 2-3](#)
- [Collecting Configurations, page 2-4](#)
- [Monitoring Task Logs, page 2-5](#)
- [Setting Up Devices for IOS XR Support, page 2-6](#)

Creating Logical Devices

To create a logical device, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Devices**.

The Devices window appears.

Step 2 Click **Create**.

Step 3 From the drop-down list, choose **Cisco Device**.

The Create Cisco Device window appears, as shown in [Figure 2-1](#).

Figure 2-1 New Device Information

Create Cisco Device

General	
Device Host Name *	
Device Domain Name:	
Description:	
Collection Zone:	None ▾
Management IP Address:	
Interfaces:	Edit
Associated Groups	Edit
Login and Password Information	
Login User:	
Login Password:	
Verify Login Password:	
Enable User:	
Enable Password:	
Verify Enable Password:	
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:	
Community String RW:	
Additional Properties:	Show
Save Cancel	

Note: * - Required Field

149136

- Step 4** Enter all required information for this new device.
- Step 5** For Additional Properties, click **Show**.
- Step 6** 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. To do this, perform the following steps.

- Step 1** Choose **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 2-2](#).



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 2-2 Create Task

Create Task	
Name *	Collect Config 2004-01-14 (mlce3DeviceCreation)
Type:	Collect Config
Description:	Created on 2004-01-14 mlce3DeviceCreation
Task Configuration Method:	☒ Simplified ☐ Advanced (via wizard)
Note: * - Required Field	

- Step 4** Click **Next**.
- The Collect Config Task window appears, as shown in [Figure 2-3](#).

Figure 2-3 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 Select Device window appears.
- Step 6** Check to choose the desired device(s), then click **Select**.
The Collect Config Task window reappears.
- Step 7** To choose device groups associated to the task, in the Groups panel, click **Select/De Select**.
A list of available device groups appears.
- Step 8** Check to choose the desired device group(s), then click **Select**.
The Collect Config Task window reappears.
- Step 9** Set schedule and task owner, if applicable.
- Step 10** Click **Submit**.
The Tasks window appears.
- Step 11** Choose your task in the Task Name column, then click **Details** to view more information.

Monitoring Task Logs

To monitor task logs, perform the following steps.

- Step 1** Choose **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 Device Groups

To create device groups, perform the following steps.

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

Setting Up Devices for IOS XR Support

ISC supports provisioning of basic MPLS VPNs on devices running Cisco's IOS XR software. IOS XR, a new member of the Cisco IOS family, is a unique self-healing and self-defending operating system designed for always-on operation while scaling system capacity up to 92Tbps.



Note For information about specific platforms and features supported for IOS XR devices for MPLS VPN, as well as IOS XR versions supported, see the [Release Notes for Cisco IP Solution Center, 5.1](#).

To enable IOS XR support in MPLS VPN, perform the following steps.

- Step 1** Set the DCPL property **Provisioning/Service/mpls/platform/CISCO_ROUTER/IosXRConfigType** to XML.
Possible values are **CLI**, **CLI_XML**, and **XML** (the default).
- Step 2** Set the DCPL property **DCS/getCommitCLIConfigAfterDownload** to true (the default).
This allows ISC to retrieve the committed CLI configuration after an XML configuration has been downloaded. See [Viewing Configlets on IOS XR Devices, page 6-32](#) for more information.
- Step 3** Create the device in ISC as an IOS XR device, as follows:
- Create the Cisco device by choosing **Service Inventory > Inventory and Connection Manager > Devices > Create**.
The Create Cisco Device window appears.

- b. Set the OS attribute, located under Device and Configuration Access Information, to IOS_XR.

**Note**

For additional information on setting DCPL properties and creating Cisco devices, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

- Step 4** Create and deploy MPLS VPN service requests, following the procedures in this guide.

Sample configlets for IOS XR devices are provided in [Appendix A, “Sample Configlets”](#).

Creating Customers, Sites, and CPEs

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

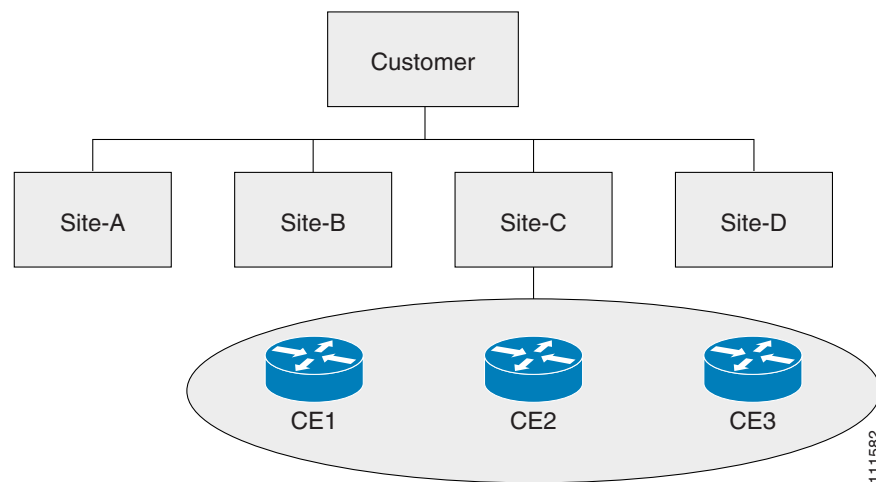
- Customer Name
- Customer Site
- Customer Device (CPE)

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 2-4](#) shows an overview of an ISC Customer.

Figure 2-4 Overview of an ISC Customer



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 covers the following topics:

- [Creating Customers, page 2-8](#)
- [Creating Sites, page 2-8](#)
- [Creating CPEs, page 2-8](#)

Creating Customers

To create a customer, perform the following steps.

-
- Step 1** Choose **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

To create a site, perform the following steps.

-
- Step 1** Choose **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

To create a CPE device, perform the following steps.

-
- Step 1** Choose **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 Select Device window appears.
- Step 5** Check to choose a device, then click **Select**.
The Create CPE Device window reappears, as shown in [Figure 2-5](#).

Figure 2-5 Create CPE Device

- 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 Providers, Regions, and PEs

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

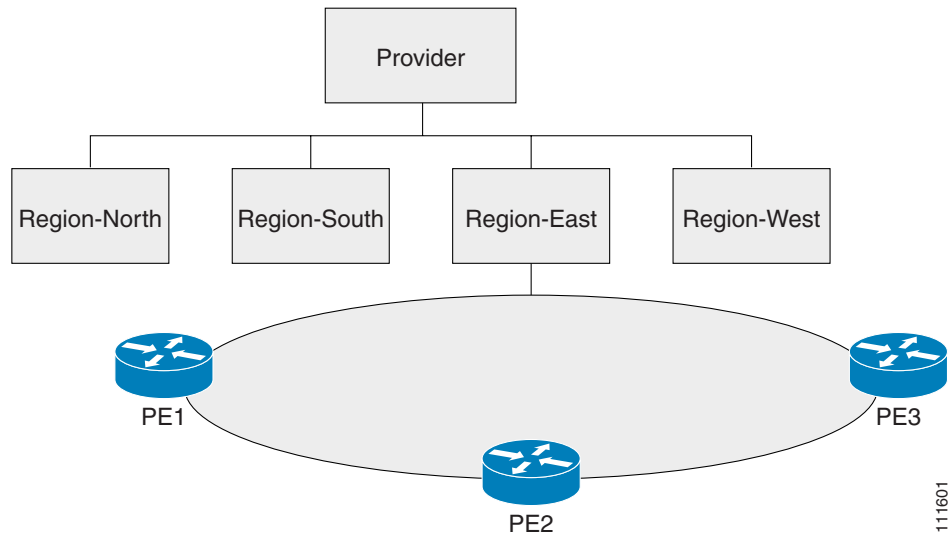
- Provider name and BGP Autonomous System (AS) number
- Provider region
- Provider edge device (PE)

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 2-6](#) shows an overview of an ISC Provider.

Figure 2-6 Overview of an ISC Provider

This section covers the following topics:

- [Creating a Provider, page 2-10](#)
- [Creating a Region for PE, page 2-11](#)
- [Creating PEs, page 2-11](#)
- [Editing PEs, page 2-12](#)

Creating a Provider

To create a provider, perform the following steps.

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

Creating a Region for PE

To create a region, perform the following steps.

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

Creating PEs

To set up a device as a Provider Edge (PE) device, perform the following steps.

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

Figure 2-7 Create PE Device

Create PE Device

Device Name *		Select
PE Region Name *		Select
PE Role Type:	N-PE ▼	6VPE: ☐

Save Cancel

Note: * - Required Field

211629

- Step 6** In the PE Region Name field, click **Select**.
The Select Region window appears.
- Step 7** Check to choose a region, then click **Select**.
The Create PE Device window reappears.
- Step 8** From the drop-down list, choose a PE Role Type (N-PE, U-PE, P, or PE-AGG).

**Note**

If the role type is N-PE, you can check the 6VPE check box to designate the device as a 6VPE device. See [Chapter 4, “IPv6 and 6VPE Support in MPLS VPN”](#) for more information on IPv6 and 6VPE support in ISC.

- Step 9** Click **Save**.
The PE Device window appears showing the PE device you have created.

Editing PEs

To view or edit a PE, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** In the Selection pane, click **PE Devices**.
The PE Devices window appears.
- Step 3** Choose the PE Device.
- Step 4** Click **Edit**.
The Edit PE Device window appears.
- Step 5** Make required changes, then click **Save**.

Creating Access Domains

**Note**

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

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

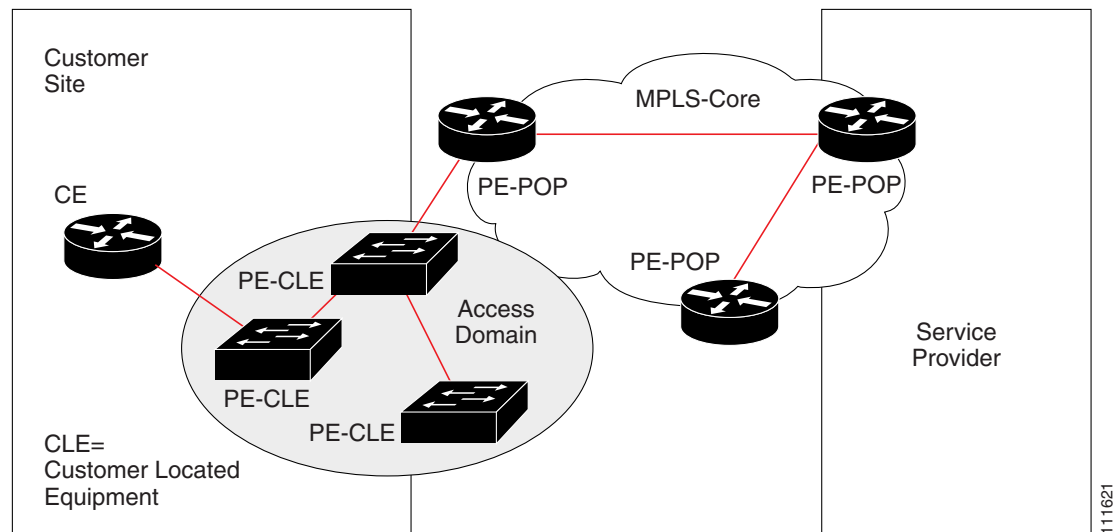
The Layer 2 Ethernet switching domain that connects a PE to a CE is called an Access Domain. All the switches attached to the PE-POP belong to this Access Domain. These switches belong to the Provider and are defined in ISC as PE-CLE.

**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 2-8](#) shows an overview of an ISC Access Domain.

Figure 2-8 Overview of an Access Domain



To create an Access Domain, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** In the Selection pane, under **Providers**, click **Access Domains**.
The Access Domains window appears.
- Step 3** Click **Create**.
The Create Access Domain window appears, as shown in [Figure 2-9](#).

Figure 2-9 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

111617

Step 4 Enter an Access Domain Name.

Step 5 Choose a Provider.

Step 6 Click **Select** to show PEs.

The Show PEs window appears.

Step 7 Choose a PE.

Step 8 Click **Select**.

You are returned to the Create Access Domain window.

Step 9 For Reserved VLANs, click **Create**.

The Create Reserved VLAN window appears, as shown in [Figure 2-10](#).

Figure 2-10 Create Reserved VLAN

Create Reserved VLAN

Starting Value*: 500 (1 - 4094)

Size*: 100 (1 - 4094)

Management VLAN: ☒

OK **Cancel**

Note: * - Required Field

111619

Step 10 Enter a Starting Value.

Step 11 Enter a Size.

Step 12 Check to choose **Management VLAN**.

Step 13 Click **OK**.

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

Creating Resource Pools

This section describes how to create Resource Pools using the Cisco IP Solution Center (ISC) GUI. It contains the following sections:

- [Overview of Resource Pools, page 2-15](#)
- [Creating an IPv4 Address Pool, page 2-16](#)
- [Creating a Multicast Pool, page 2-16](#)
- [Creating a Route Distinguisher Pool, page 2-17](#)
- [Creating a Route Target Pool, page 2-18](#)
- [Creating a Site of Origin Pool, page 2-19](#)
- [Creating a VC ID Pool, page 2-20](#)
- [Creating a VLAN Pool, page 2-21](#)

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:

- **IPv4 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.
- **Virtual Circuit Identifier (VC ID)**—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.

**Note**

The VLAN pool does not supply a value for a second VLAN ID, when that feature is used for Q-in-Q matching. See the section [Notes on the VLAN ID and Second VLAN ID Attributes, page 6-10](#) for additional information about second VLAN ID.

Creating an IPv4 Address Pool

To create an IPv4 address pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **IPv4 Address** from the Pool Type drop-down list.

Step 3 Click **Create**.

The Create IP Address Pool window appears, as shown in [Figure 2-11](#).

Figure 2-11 Create IP Address Pool

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

111641

Step 4 Enter an IP Address and Mask.

Step 5 Choose the **Pool Mask (bits)** value (30).



Note Use 32 for loopback addresses.

Step 6 Click **Select** to associate the pool to a Region.

The Select Region window appears.

Step 7 Choose a **Region**.

Step 8 Click **Select**.

The Create IP Address Pool window reappears.

Step 9 Click **Save**.

The Resource Pools - IP Address window appears showing that the IP Address Pool is in the Repository.

Creating a Multicast Pool

To create a multicast pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

- Step 2** Choose **Multicast** from the Pool Type drop-down list.
The Resource Pools - Multicast window appears.
- Step 3** Click **Create**.
The Create Multicast Pool window appears, as shown in [Figure 2-12](#).

Figure 2-12 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

111646

- Step 4** Enter an IP Address and Mask.
- Step 5** Choose the defaults (**Default MDT** and **Data MDT**).
- Step 6** Click **Save**.
The Resource Pools - Multicast window appears showing the Multicast Address Pool in the Repository.

Creating a Route Distinguisher Pool

To create a route distinguisher (RD) pool, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.
The Resource Pools window appears.
- Step 2** Choose **Route Distinguisher** from the Pool Type drop-down list.
The Resource Pools - Route Distinguisher window appears.
- Step 3** Click **Create**.
The Create Route Distinguisher Pool window appears, as shown in [Figure 2-13](#).

Figure 2-13 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 4 Enter an RD Pool Start value.

Step 5 Enter an RD Pool Size value.

Step 6 Click **Select**.

The Select Provider window appears.

Step 7 Choose a **Provider**.

Step 8 Click **Select**.

The Create Route Distinguisher Pool window reappears.

Step 9 Click **Save**.

The Resource Pools - Route Distinguisher window appears showing the Route Distinguisher Pool in the Repository.

Creating a Route Target Pool

To create a route target (RT) pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **Route Target** from the Pool Type drop-down list.

The Resource Pools - Route Target window appears.

Step 3 Click **Create**.

The Create Route Target Pool window appears, as shown in [Figure 2-14](#).

Figure 2-14 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 4 Enter an RT Pool Start value.

Step 5 Enter an RT Pool Size value.

Step 6 Click **Select**.

The Select Provider window appears.

Step 7 Choose a **Provider**.

Step 8 Click **Select**.

The Create Route Target Pool window reappears.

Step 9 Click **Save**.

The Resource Pools - Route Target window appears showing the Route Target Pool in the Repository.

Creating a Site of Origin Pool

To create a site of origin (SOO) pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **Site of Origin** from the Pool Type drop-down list.

The Resource Pools - Site of Origin window appears.

Step 3 Click **Create**.

The Create Site of Origin Pool window appears, as shown in [Figure 2-15](#).

Figure 2-15 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

11:16:30

Step 4 Enter an SOO Pool Start value.

Step 5 Enter an SOO Pool Size value.

Step 6 Click **Select**.

The Select Provider window appears.

Step 7 Choose a **Provider**.

Step 8 Click **Select**.

The Create Site of Origin Pool window reappears.

Step 9 Click **Save**.

The Create Route Target Pool window appears showing a Site of Origin Pool in the Repository.

Creating a VC ID Pool

To create a VC ID pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **VC ID** from the Pool Type drop-down list.

The Resource Pools - VC ID window appears.

Step 3 Click **Create**.

The Create VC ID Pool window appears, as shown in [Figure 2-16](#).

Figure 2-16 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

Step 4 Enter an VC Pool Start value.

Step 5 Enter an VC Pool Size value.

Step 6 Click **Save**.

The Resource Pools - VC ID window appears showing a VC ID Pool in the Repository.

Creating a VLAN Pool

To create a VLAN pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **VLAN** from the Pool Type drop-down list.

The Resource Pools - VLAN window appears.

Step 3 Click **Create**.

The Create VLAN Pool window appears, as shown in [Figure 2-17](#).

Figure 2-17 VLAN Pool

Create VLAN Pool

VLAN Pool Start *: 500 (1 - 4094)

VLAN Pool Size *: 100 (1 - 4094)

Access Domain *: Select

Save Cancel

Note: * - Required Field

Step 4 In the VLAN Pool Start field, enter a valid value.

Step 5 In the VLAN Pool Size field, enter a valid value.

- Step 6** Choose an access domain by clicking **Select**.
The Select Access Domain window appears.
- Step 7** Choose an **Access Domain**.
- Step 8** Click **Select**.
The Create VLAN Pool window reappears.
- Step 9** Click **Save**.
The Resource Pools - VLAN window appears showing the VLAN Pool in the Repository.

**Note**

The VLAN pool does not supply a value for a second VLAN ID, when that feature is used for Q-in-Q matching. See the section [Notes on the VLAN ID and Second VLAN ID Attributes, page 6-10](#) for additional information about second VLAN ID.

Defining VPNs

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 can be defined within ISC.

**Note**

It is also possible to specify VPN and VRF information in an independent VRF object, which is subsequently deployed to a PE device and then associated with an MPLS VPN link via an MPLS VPN service request. For details on using this feature, see [Chapter 3, “Independent VRF Management.”](#)

This section describes how to define MPLS VPNs and IP Multicast VPNs. It contains the following sections:

- [Creating an MPLS VPN, page 2-22](#)
- [Creating an IP Multicast VPN, page 2-26](#)
- [Enabling a Unique Route Distinguisher for a VPN, page 2-28](#)

Creating an 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 framework that provides private IP networking over a public infrastructure such as the Internet. In Cisco 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 an MPLS VPN, perform the following steps.

-
- Step 1** Click the **Service Inventory** tab.
- Step 2** Choose **Inventory and Connection Manager**.
The Inventory and Connection Manager window appears.
- Step 3** From the Inventory and Connection Manager window, choose **VPNs**.
The VPNs window appears.
- Step 4** From the VPNs window, click **Create**.
The Create VPN window appears, as shown in [Figure 2-18](#).

Figure 2-18 Create VPN

Create VPN

Name * :

Customer * : [Select](#)

MPLS Attributes

Create Default CE Routing Community: ☐

Enable Unique Route Distinguisher: ☐

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:

MDT MTU: (576 - 18010)

Enable PIM SSM: ☐

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 Go of 1			

CE Routing Communities: [Select](#) [Remove](#)

VPLS Attributes

Enable VPLS: ☐

VPN ID: (1-2147483646)

Service Type:

Topology:

[Save](#) [Cancel](#)

211613

Step 5 Name: Enter the name of the VPN.

Step 6 Customer: To choose the customer associated with this VPN:

- a. Click **Select**.

The Select Customer dialog box appears.

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

The Create VPN window reappears.

- Step 7 Create Default CE Routing Community:** To create a default CE routing community, check the **Create Default CE Routing Community** check box and choose a provider.
- Step 8 Enable Unique Route Distinguisher:** For coverage of this attribute see [Enabling a Unique Route Distinguisher for a VPN, page 2-28](#).
- Step 9 Enable Multicast:** To enable multicast for the VPN, see [Creating an IP Multicast VPN, page 2-26](#).
- 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 2-32](#)).



Note You must specify a CERC if multicast is enabled.

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

The Select CE Routing Communities dialog box appears.

- b. Check 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, as shown in [Figure 2-19](#).

Figure 2-19 New CERC Selected

The screenshot shows the 'Create VPN' dialog box with the following settings:

- 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) [Select] [Remove]
- VPLS Attributes:**
 - Enable VPLS: ☐
 - Service Type: ERS
 - Topology: Full Mesh

Buttons at the bottom: Save, Cancel.

- 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 CE's 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 an IP Multicast VPN

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 [Creating a Multicast Pool, page 2-16](#), for further information.


Note

If the multicast VPN is used in a service request for IPv4 on a device running IOS XR, not all of the multicast attributes in the Create VPN window are supported. This is because there is not a one-to-one mapping of IOS multicast commands to IOS XR commands. These exceptions are noted in the following steps. For a comparison of multicast routing commands in IOS and IOS XR, see [Multicast Routing on IOS XR Devices, page 4-6](#).


Note

Multicast VRF deployments are supported only for IPv4 deployments. They are not supported for either IPv6 or IPv4+IPv6 modes. For more information about VRF object support in ISC, see [Chapter 3, “Independent VRF Management.”](#)

To create an IP Multicast VPN, follow the procedure described in [Creating an MPLS VPN, page 2-22](#) to the place where you can enable multicast for the VPN, then perform the following steps.

- Step 1** To enable multicast for the VPN, check **Enable Multicast**.
The current window refreshes with additional fields becoming active.
- Step 2** 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 3** From the drop-down list, choose a value for Data MDT Size.
- Step 4** In the next field, enter a valid value for Data MDT Threshold (1 - 4294967 kilobits/sec).
- Step 5** 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.

**Note**

For IOS XR devices, when SPARSE_DENSE_MODE is chosen, no configlet will be generated. Sparse-dense mode is not supported by IOS XR, only sparse mode (default) and bidirectional mode. For IOS XR devices, sparse mode is running by default when multicast routing is enabled on an interface. Hence, no configlet will be generated for sparse mode either.

Step 6 In the next field, enter a valid value for MDT MTU (Maximum Transmission Unit).

**Note**

The ranges for IOS and IOS XR devices for this attribute are different. The range for IOS devices is from 576 to 18010, and for IOS XR devices it is from 1401 to 65535. Device type validations are done during service request creation when it is known what type of device the multicast VPN will be deployed on.

Step 7 To enable PIM SSM (Source Specific Multicast), check the associated check box.

When you check the check box:

- a. 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**.

**Note**

For IOS XR devices, when DEFAULT is chosen, no configlet will be generated because this command is running by default on IOS XR devices, using the standard SSM range 232.0.0.0/8.

- b. 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 8 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 9 In the next field enter a valid value for the Multicast Route Limit (1 - 2147483647).

**Note**

For IOS XR devices, no configlet is generated for this attribute. The command to set the route limit per VRF is not supported on IOS XR devices.

Step 10 To enable the auto RP (Rendezvous Point) listener function, check the associated check box.

**Note**

For IOS XR devices, no configlet is generated for this attribute. By default, this feature is running on IOS XR devices.

Step 11 To configure Static RPs, check the associated check box.

When you check this, the Edit option for PIM Static RPs goes active.

Step 12 To edit or add PIM Static RPs, click **Edit**.

The Edit PIM Static RPs window appears, as shown in [Figure 2-20](#).

Figure 2-20 Edit PIM Static RPs

#	☐	Static-RP Unicast Address	Multicast-Group List Name	Override
1.	☐	10.99.1.1	rpl1List	☒
2.	☐	10.99.1.2	rpl2List	☐
3.	☐	10.99.1.5		☒

Showing 1 - 3 of 3 records

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

Add Delete OK Cancel

Step 13 Complete all applicable fields in the Edit PIM Static RP window, then click **OK**.

The data now appears in the main Create VPN window.

Step 14 To save your changes and add this Multicast VPN to you system, at the bottom of the window, click **Save**.

Enabling a Unique Route Distinguisher for a VPN



Note

In ISC 5.1, enabling unique route distinguishers is only supported for IOS devices. It is not supported for IOS XR devices.

Support for multipath load sharing requires unique route distinguishers (RDs) for each PE router for a VPN (VRF). This is to prevent the same RDs from being allocated to different customers. This allows the use of the same RD for the same VRF. That is, all sites in the PE can have the same unique RD. The unique RD feature is optional. It is enabled at both a global VPN level or a service request level. To enable the unique RD per PE for a VPN, the Create VPN window contains the attribute **Enable Unique Route Distinguisher** field.

Each VPN deployed through ISC for which **Enable Unique Route Distinguisher** has been selected is marked as a multipath VPN. This ensures a unique RD allocation for each VRF on each PE. Enabling multipath for an already deployed VPN creates new VRFs on all the PEs of the VPN and assigns a unique RD. When **Enable Unique Route Distinguisher** is selected for the VPN, the **Allocate New Route Distinguisher** and **VRF and RD Overwrite** attributes will be disabled when setting up a policy or service request that uses this VPN.

To use the unique RD feature, perform the following steps.

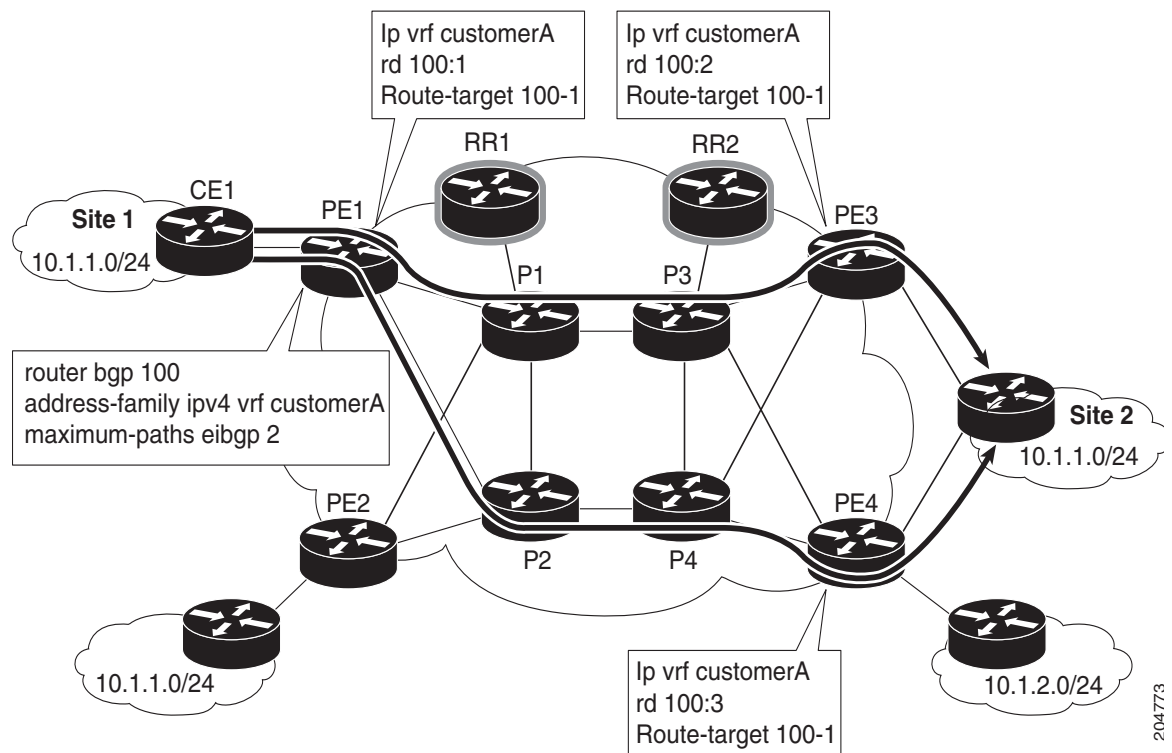
-
- Step 1** When creating a VPN, check the **Enable Unique Route Distinguisher** check box.
- Step 2** When subsequently creating a service policy and/or service request, select the VPN in the VRF and VPN Membership window.
- The Unique Route Distinguisher **field** appears.
- Step 3** If the unique RD allocation functionality is required, check the **Unique Route Distinguisher** check box.
-

For additional information on how this feature is used with MPLS VPN policies and service requests, see [Defining VRF and VPN Information](#), page 5-29.

Provisioning MPLS Service Requests Using Unique Route Distinguisher

The unique route distinguisher (RD) feature is used to implement multipath load balancing. Multihomed CEs often require load balancing across multiple available paths. In a full-mesh BGP environment, PEs receive all the available paths to a given prefix, and load balancing can easily be achieved. However, when route reflectors are present in the service provider core, PE routers receive only one route, even if multiple paths exist, and load balancing does not occur. To achieve load balancing, the service provider needs to implement unique RD values for the customer VPN on each PE router. In addition, eBGP configuration with the desired number of paths (across which load balancing is desired) needs to be enabled in the service provider environment. [Figure 2-21](#) illustrates a load balancing example.

Figure 2-21 Load Balancing Using Different RDs



204773

The support for multipath load sharing requires unique RDs for each PE router for a VPN (VRF). This is to prevent the same RDs from being allocated to different customers. This allows the use of the same RD for the same VRF. That is, all sites in the PE can have the same unique RD. The unique RD feature is optional. You can specify its use at both the policy or service request level.

It is enabled at both a global VPN level or a service request level.

ISC supports BGP multipath load sharing through fields and options in the ISC GUI. The following steps provide an overview of how to do this.

- Step 1** When creating a VPN, check the **Enable Unique Route Distinguisher** check box in the Create VPN window, as shown in [Figure 2-22](#).

Figure 2-22 Enabling Unique RD in Create VPN

Create VPN	
Name *	vpn_1
Customer *	Select
MPLS Attributes	
Create Default CE Routing Community:	☐ Provider1 ▼
Enable Unique Route Distinguisher:	☒
Enable Multicast: ⓘ	☐

For some additional coverage of this, see [Enabling a Unique Route Distinguisher for a VPN](#), page 2-28.

- Step 2** When setting the attributes in the policy (MPLS Policy Editor - VRF and VPN Membership window) or service request (MPLS Link Attribute Editor - VRF and VPN window), use the **BGP Multipath Load Sharing** check box to enable or disable BGP multipath load sharing.

Enabling BGP multipath load sharing by checking the check box causes additional attributes to appear in the GUI. For detailed coverage of these attributes and how to set them, see [BGP Multipath Load Sharing and Maximum Path Configuration](#), page 5-32.

- Step 3** When creating a service request based on this policy, check the **Unique Route Distinguisher** check box in the MPLS Link Attribute Editor - VRF and VPN window, as shown in [Figure 2-23](#).

Figure 2-23 Enabling Unique Route Distinguisher in a Service Request

MPLS Link Attribute Editor - VRF and VPN

Attribute	Value				
VRF Information					
Use VRF Object:	☐				
Export Map:					
Import Map:					
Maximum Routes:	(1-4294967295)				
Maximum Route Threshold *:	80 (1-100)				
VRF Description:					
BGP Multipath Load Sharing:	☐				
Unique Route Distinguisher:	☒				
Allocate New Route Distinguisher:	☐				
VRF And RD Overwrite:	☐				
VPN Selection					
PE VPN Membership *:					
Select	Customer	VPN	Provider	CERC	Is Hub
☐	Customer1	vpn_3	Provider1	CERC_1	☒
Add Delete					

Note: * - Required Field

204775

**Note**

The Unique Route Distinguisher attribute is dynamic and only shows up in the GUI if a VPN with unique RD enabled is selected.

Step 4

Complete the service request creation, and save the service request.

Use Cases for Using Unique RD

The following use cases demonstrate the behavior of unique RD feature.

Use case details:

- The default values of the VPN/VRF are:

```
ip vrf V24:unique2
rd 1:33
route-target import 1:14
route-target import 1:15
route-target export 1:14
```

- Service requests are created using PEs and enabling or disabling the Unique RD attribute during service request creation, as shown in [Table 2-1](#).
- The outcomes for various cases are described in the Results column of the table.

Table 2-1 Unique RD Use Cases

SR #	PE	Unique RD	VRF:RD	Results
1	pe1	False	V24:33	ISC uses the default <i>vrfName:RD</i> , because this is the first time this PE has been configured with this <i>vrfName:RD</i> name.
2	pe2	False	V24:33	ISC uses the default <i>vrfName:RD</i> .
3	pe3	True	V25:34	ISC creates a new <i>vrfName:RD</i> , because Unique RD is true, and it is on a different PE. This PE (pe3) did not have this <i>vrfName:RD</i> configured.
4	pe3	True	V25:34	ISC uses the <i>vrfName:RD</i> from SR #3, because the new RD is already present on the PE router.
5	pe2	True	V26:35	ISC creates a new <i>vrfName:RD</i> , because this is the first time Unique RD is selected as true, even though a VRF of V24:33 was already configured in SR #2.
6	pe1	True	V27:36	ISC creates a new <i>vrfName:RD</i> , because this is the first time Unique RD is selected as true on this PE, even though a VRF of V24:33 was already configured in SR #1.
7	pe1	False	V24:33	ISC uses the default <i>vrfName:RD</i> , as in SR #1.
8	pe3	False	V24:33	ISC uses the default <i>vrfName:RD</i> , as in SR #1.
9	pe3	True	V25:34	ISC uses the newly created <i>vrfName:RD</i> in SR #4, because it already created a new <i>vrfName:RD</i> for this PE.
10	pe2	True	V26:35	ISC uses the newly created <i>vrfName:RD</i> in SR #5, because it already create a new <i>vrfName:RD</i> for this PE.
11	pe1	True	V27:36	ISC uses the newly create <i>vrfName:RD</i> in SR #6, because it already create a new <i>vrfName:RD</i> for this PE.

Creating CE Routing Communities

CE Routing Communities (CERCs) are the means by which 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. 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, perform the following steps.

-
- Step 1** Click the **Service Inventory** tab.
- Step 2** Choose **Inventory and Connection Manager**.
The Inventory and Connection Manager window appears.
- Step 3** Choose **CE Routing Communities**.
The CE Routing Communities window appears.
- Step 4** Click **Create**.
The Create CE Routing Community window appears, as shown in [Figure 2-24](#).

Figure 2-24 Defining a New CE Routing Community

- Step 5** Complete the CERC fields as required for the VPN:
- Provider: To specify the service provider associated with this CERC, click **Select**.
The Select Provider dialog box appears.
 - Choose the name of the service provider, then click **Select**.
 - Name: Enter the name of the CERC.
 - CERC Type: Specify the CERC type: Hub and Spoke or Fully Meshed.
 - 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.



Note If you choose to bypass the **Auto-pick route target values** option and set the route target (RT) values manually, 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**.
-



CHAPTER 3

Independent VRF Management

This chapter describes independent VRF management, which provides a means to create, deploy and manage VRF objects independent of MPLS VPN links and service requests. Deployed VRF objects can also be used with MPLS VPN links. It contains the following sections:

- [Overview, page 3-1](#)
- [Working with VRF Objects, page 3-2](#)
- [Working with VRF Service Requests, page 3-11](#)
- [Using VRFs with MPLS VPN Service Requests and Policies, page 3-16](#)
- [Migrating Existing MPLS VPN Service Requests to the VRF Object Model, page 3-21](#)

Overview

In the traditional VRF (VPN routing and forwarding) model available in previous releases of ISC, the operator first creates a VPN object and then associates it to an MPLS VPN link. The necessary VRF information is generated and deployed at the time the MPLS VPN link is provisioned. The VRF information is removed only when the last link associated with the VRF is decommissioned. However, in certain cases, it might be desirable to have the VRF information provisioned independent of the physical link. ISC now supports this scenario through the independent VRF management feature described in this chapter. This lets you create, modify, and delete VRF objects independently of MPLS VPN links. This provides several advantages:

- VRF information and templates can be directly deployed on a PE device without being associated with an interface.
- VRF information can exist without links pointing to it.
- A VRF object can be modified, even if it is associated with links.
- Route targets (RTs) can be added and removed without causing outages.

Managing VRFs independently of physical links involves the following tasks, which are covered in detail in the rest of this chapter:

- Creating, modifying, and deleting VRF objects.
- Creating, modifying, deploying, decommissioning, and deleting a new type of service request, called a VRF service request.
- Using deployed VRF objects with MPLS VPN links via service policies and service requests.
- Migrating traditional MPLS VPN service requests to the independent VRF model.

**Note**

The traditional ISC VRF model is still supported for backward compatibility. The choice of which VRF model to use is available during MPLS VPN link creation. This is described in subsequent sections of this chapter.

Working with VRF Objects

This section describes how to create, modify, and delete VRF objects. Subsequent sections in this chapter cover how the VRF objects are used in service requests. This section covers the following topics:

- [Creating a New VRF Object, page 3-2](#)
- [Copying a VRF Object, page 3-5](#)
- [Searching for VRF Objects in the ISC Repository, page 3-7](#)
- [Modifying Non-Deployed VRF Objects, page 3-7](#)
- [Modifying Deployed VRF Objects, page 3-9](#)
- [Deleting VRF Objects, page 3-10](#)

Creating a New VRF Object

Creating a VRF object is similar to creating a VPN. However, there are some extra attributes involved, such as Import RT List and Export RT List. After the VRF object is created, you will later provision it using a VRF service request, as covered in later sections of this chapter.

To create a VRF object, perform the following steps.

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

The Inventory and Connection Manager window appears.

Step 2 From the Inventory and Connection Manager, choose **VRFs**.

The VRF Management window appears, as shown in [Figure 3-1](#).

Figure 3-1 VRF Management Window

#	VRF Name	Provider
1.	VRF_1	Provider1
2.	VRF_2	Provider1

Step 3 From the VRF Management window, click **Create**.

The Create VRF window appears, as shown in [Figure 3-2](#).

Figure 3-2 Create VRF Window

Create VRF

Name *	
Provider *	Select
Description:	

VRF Attributes

CE Routing Communities *	Select								
Import RT List:									
Export RT List:									
Import Route Map:									
Export Route Map:									
Maximum Routes: ⓘ	(1 - 4294967295)								
Threshold: ⓘ	(1 - 100)								
RD *	☐ Autopick RD								
Enable Multicast: ⓘ	☐								
Enable Auto Pick MDT Addresses:	☒								
Default MDT Address *	(a.b.c.d)								
Data MDT Subnet *	(a.b.c.d)								
Data MDT Size:	1								
Data MDT Threshold:	(1 - 4294967 kilobits/sec)								
Default PIM Mode:	SPARSE_DENSE_MODE								
MDT MTU: ⓘ	(576 - 65535)								
Enable PIM SSM:	☐ DEFAULT								
SSM List Name *									
Multicast Route Limit:	(1 - 2147483647)								
Enable Auto RP Listener:	☐								
Configure Static-RP:	☐								
My PIM Static-RPs *	Showing 0 of 0 records Edit <table border="1"> <thead> <tr> <th>#</th> <th>Static-RP Unicast Address</th> <th>Multicast-Group List Name</th> <th>Override</th> </tr> </thead> <tbody> <tr> <td colspan="4">Rows per page: 10 Go to page: 1 of 1 Go </td> </tr> </tbody> </table>	#	Static-RP Unicast Address	Multicast-Group List Name	Override	Rows per page: 10 Go to page: 1 of 1 Go			
#	Static-RP Unicast Address	Multicast-Group List Name	Override						
Rows per page: 10 Go to page: 1 of 1 Go									

211668

Step 4 Name: Enter the name of the VRF object.

This is a simple text field. Enter any name of your choice. It is recommended not to use special characters (' ` " < > () [] { } / \ & ^ ! ? ~ * % = , . + |), as this may cause misconfiguration of the VRF name for certain devices.

This name will be directly deployed on the PE device. All the validations applicable for a VPN name while creating a VPN object in ISC are applicable for a VRF name. This attribute is required.

- Step 5 Provider:** To choose the provider associated with this VRF:
- Click **Select**.
The Select Provider dialog box appears.
 - From the list of providers, choose the appropriate provider, then click **Select**.
The Create VRF window reappears.
- This attribute is required.
- Step 6 Description:** Enter a description of the VRF, if desired.
No validation is done on the description entered.
- Step 7 CE Routing Communities:** To select a CE routing community (CERC) for this VRF:
- Click **Select**.
The Select CE Routing Communities dialog box appears.
 - From the list of CERCs, choose the appropriate CERC, then click **Select**.
Only one CERC is allowed per VRF. The Create VRF window reappears.
- This attribute is required.
- Step 8 Import RT List:** Enter one or more Route Targets (RTs) to be imported in the VRF.
For multiple RTs, use a comma (,) separated list. An example RT list is 100:120,100:130,100:140.
- Step 9 Export RT List:** Enter one or more Route Targets (RTs) to be exported from the VRF.
For multiple RTs, use a comma (,) separated list.
- Step 10 Import Route Map:** Enter the name of a route map defined on the device.
ISC will validate this name while provisioning the VRF. If the route map is not defined, ISC will generate an error.
- Step 11 Export Route Map:** Enter the name of a route map defined on the device.
ISC will validate this name while provisioning the VRF. If the route map is not defined, ISC will generate an error.
- Step 12 Maximum Routes:** Specify the maximum number of routes that can be imported into the VRF.
This is an integer value from 1 to 4294967295 for IOS devices and from 32 to 2000000 for IOS XR devices.
- Step 13 Threshold:** Specify the threshold value, which defines a percentage, which, if exceeded, generates a warning message.
This is an integer value from 1 to 100. This attribute is mandatory for IOS devices and optional for IOS XR devices. Validations for specific device type will be done during service request creation.
- Step 14 RD:** Specify a RD (route distinguisher) manually, or check the **Autopick RD** check box to have ISC automatically choose an RD from the Route Distinguisher pool (if one has been set up).
This attribute is required.
- Step 15 Enable Multicast:** Check this check box to enable multicast VRF.
The multicast attributes below this check box are enabled for use. For details on how to set the multicast attributes, see [Creating an IP Multicast VPN, page 2-26](#), starting with Step 2 in the procedure.

**Note**

Multicast VRF deployments are supported only for IPv4 deployments. CERC is mandatory if multicast is enabled.

**Note**

For the MDT MTU attribute: The range for IOS devices is from 576 to 18010. The range for IOS XR devices is from 1401 to 65535. Validations for specific device type will be done during service request creation.

Step 16 When you are satisfied with the settings for this VRF object, click **Save**.

ISC creates a new VRF object based the attributes selected. The VRF Management window appears. The new VRF is listed in the VRF Name column of the window.

Copying a VRF Object

You can use an existing VRF object as the basis for a new one. You do this by copying a VRF object, renaming the copy, and (optionally) modifying its attributes.

To copy an existing VRF object, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > VRF management**.

The VRF Management window appears, as shown in [Figure 3-3](#).

Figure 3-3 VRF Management Window

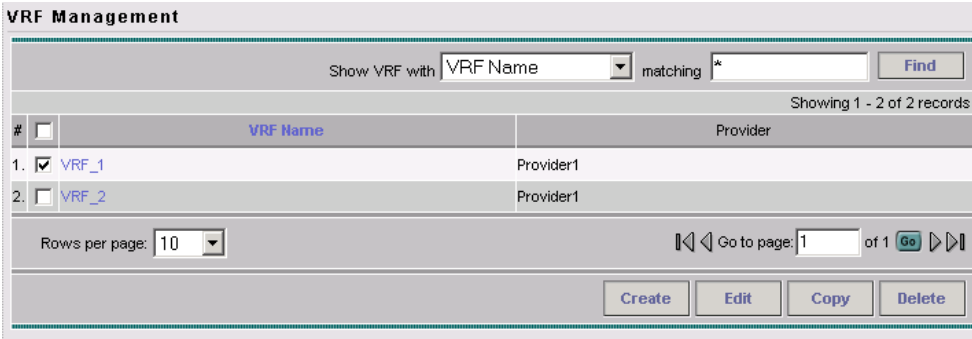
The screenshot shows the 'VRF Management' window. At the top, there is a search bar with 'Show VRF with' and a dropdown menu set to 'VRF Name', followed by a text input field with an asterisk and a 'Find' button. Below the search bar, it says 'Showing 1 - 2 of 2 records'. The main area contains a table with two columns: 'VRF Name' and 'Provider'. There are two rows of data: '1. VRF_1' with 'Provider1' and '2. VRF_2' with 'Provider1'. Each row has a checkbox to its left. At the bottom of the table, there is a 'Rows per page' dropdown set to '10' and a pagination control showing 'Go to page: 1 of 1' with 'Go' and navigation arrows. At the very bottom, there are four buttons: 'Create', 'Edit', 'Copy', and 'Delete'.

**Note**

The example assumes that a VRF object has already been created. See [Creating a New VRF Object, page 3-2](#) for information on how to create a VRF object.

Step 2 Select an existing VRF object (for example, VRF_1) by checking the check box for the VRF object.

When you select a VRF object, the Edit, Copy, and Delete buttons become active, as shown in [Figure 3-4](#).

Figure 3-4 VRF Object Selected in the VRF Management Window


VRF Management

Show VRF with matching

Showing 1 - 2 of 2 records

#	☐	VRF Name	Provider
1.	☒	VRF_1	Provider1
2.	☐	VRF_2	Provider1

Rows per page: Go to page: of 1

Step 3 To copy the VRF object, click the **Copy** button.

The Create VRF window appears. The attribute fields are populated with values from the VRF object being copied.

Step 4 Provide a name for the new VRF object by changing the name in the **Name** field.

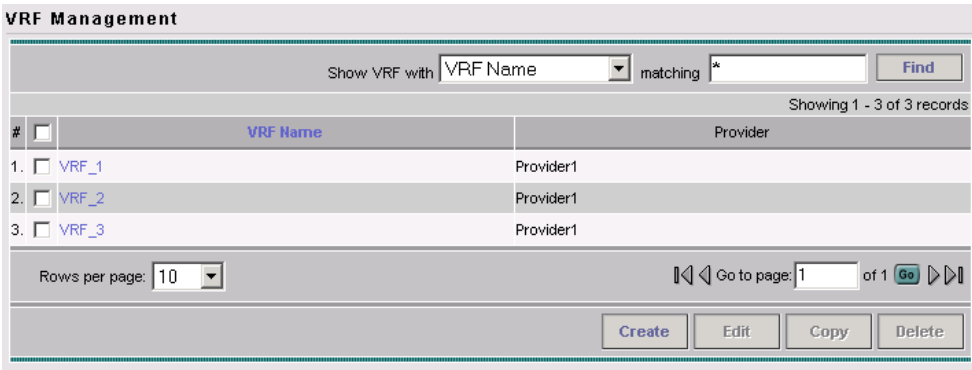
Step 5 Edit other attributes in the Create VRF window as desired.

**Note**

The copy VRF function copies all attributes of the parent except the route distinguisher (RD), Default MDT Address, and Data MDT Subnet. The RD is always set to auto pick (the Autopick RD check box is checked by default). If auto pick is set for the parent VRF, it will be carried to the VRF object created by the copy function.

Step 6 When you are finished with the edits, click the **Save** button.

The VRF Management window appears, with the new VRF object (VRF_3) displayed, as shown in [Figure 3-5](#).

Figure 3-5 New VRF Object Displayed in the VRF Management Window


VRF Management

Show VRF with matching

Showing 1 - 3 of 3 records

#	☐	VRF Name	Provider
1.	☐	VRF_1	Provider1
2.	☐	VRF_2	Provider1
3.	☐	VRF_3	Provider1

Rows per page: Go to page: of 1

Step 7 The VRF object copy operation is complete.

Searching for VRF Objects in the ISC Repository

All VRF objects are stored in the ISC repository. You can display these by accessing the VRF Management window at **Service Inventory > Inventory and Connection Manager > VRFs** in the ISC GUI. You can search for VRF objects using the **Show VRF with** drop-down list together with the **matching** field. The **Show VRF with** drop-down list enables you to display VRF objects by searching for these attributes:

- VRF Name
- Provider
- Route Distinguisher
- Route Target
- CERC

**Note**

The search is case insensitive, and wildcard (*) searches are supported.

Modifying Non-Deployed VRF Objects

VRF objects can be modified individually (single VRF edit) or in batch mode (multi-VRF edit). This section covers the basic steps for modifying VRF objects which have not yet been deployed via a VRF service request or associated with MPLS VPN links. There are some special considerations when modifying VRFs which have been deployed, as described in [Modifying Deployed VRF Objects, page 3-9](#).

Single-VRF Edit Mode

To edit one VRF object, perform the following steps.

Step 1	Choose Service Inventory > Inventory and Connection Manager > VRF management to list the VRF objects in the ISC repository. The VRF Management window appears.
Step 2	Select the VRF you want to edit and click the Edit button. The VRF Edit window appears. This window is similar to the Create VRF window shown in Figure 3-2 .
Step 3	Update any attributes you want to edit.
Step 4	Click Save to save the edits.

Multi-VRF Edit Mode

The multi-VRF edit feature allows you to modify common attributes on more than one VRF. For example, multi-VRF edit is useful for adding and/or removing route targets on multiple VRFs.

To edit multiple VRF objects simultaneously, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > VRF management** to list the VRF objects in the ISC repository.

The VRF Management window appears.

Step 2 Select the VRFs you want to edit and click the **Edit** button.

The Edit VRFs window appears, as shown in [Figure 3-6](#).

Figure 3-6 Edit VRFs

Edit VRFs

VRF'S Affecting		
VRF Details	VRF_1 ,VRF_2	Attributes

Route Attributes		
	Import Targets	Export Targets
Add		
Remove		
Provider:	Provider1	
CE Routing Communities:		Select
Import Route Map:		
Export Route Map:		

Multicast Attributes	
Enable Multicast: ⓘ	☐
Data MDT Size:	0 ▾
Data MDT Threshold:	(1 - 4294967 kilobits/sec)
Default PIM Mode:	SPARSE_DENSE_MODE ▾
MDT MTU: ⓘ	(576 - 65535)
Enable PIM SSM:	☐ DEFAULT ▾
SSM List Name *	
Multicast Route Limit:	(1 - 2147483647)
Enable Auto RP Listener:	☐

211640

The Edit VRFs window is similar to the Create VRF and Edit VRF windows. However, there is an additional field, **VRF Details**, and the format of the RT import/export fields are laid out differently. Also, some attributes are not available for editing in multi-VRF edit mode.

Step 3 To see details of the VRFs being edited, click the **Attributes** link in the VRF Details row.

The VRF Details window appears. This lists the VRFs being edited and displays the following attributes for each VRF:

- Name
- Provider
- CERC
- Import Route Map

- Export Route Map
- Import Route Target
- Export Route Target
- MultiCast

Step 4 To add or remove import or export route maps, enter the desired values in the provided fields. You can enter more than one RT in each field. For multiple RTs, use a comma (,) separated list.

Step 5 Update the **CE Routing Communities**, **Import Route Map**, **Export Route Map**, and **Multicast Attributes** settings as desired.



Note The **Provider** attribute cannot be edited in multi-VRF editing mode.

Step 6 To save the edits, click **Save**.

Modifying Deployed VRF Objects

After a VRF object is deployed on a PE device through a VRF service request (see [Deploying VRF Service Requests, page 3-13](#)), there are some special considerations to be aware of when modifying the VRF object.

- The VRF object might have been associated with multiple links and/or VRF service requests.
- Unlike traditional VPN objects, you can modify a VRF object even if it is referenced by multiple VRF service requests.
- The **VRF Name**, **Provider**, and **RD** attributes cannot be changed after the VRF object is deployed.



Note The **RD** attribute can be modified if the VRF service request is deployed on a PE device running IOS 12.0 (32) SY or greater.

To modify a deployed VRF object, perform the following steps.

Step 1 When you attempt to modify a deployed VRF object, the Affected Jobs window appears, as shown in [Figure 3-7](#).

Figure 3-7 Affected Jobs Window

Job ID	SR ID	Link ID	VRF	Description
15	17	11	VRF_1	

Showing 1 - 1 of 2 records

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

Save Save and Deploy Cancel

The window displays the affected VRF service requests associated with the VRF object being modified. The Job ID, SR ID, Link ID, VRF Name, and Description information for each VRF service request are listed.

- Step 2** To display more details about a VRF service request, click the **Job ID** link.
The Service Request Details window appears.
- Step 3** Verify the service request details, if desired.
- Step 4** Perform one of the following actions:
- Click **Save** to save the VRF object and move all of the affected VRF service requests to the REQUESTED state.
 - Click **Save and Deploy** to save the VRF object, move all of the affected VRF service requests to the REQUESTED state, and schedule an immediate deployment for all of the VRF service requests.
 - Click **Cancel** to cancel the operation and return to the Edit VRFs window.

Deleting VRF Objects

To delete VRF objects from the ISC repository, perform the following steps.



Note

There are some prerequisite steps you must perform if the VRF object or objects are still in use by a VRF service request, as mentioned in the notes following the procedure.

- Step 1** Click the **Service Inventory** tab.
- Step 2** Choose **Inventory and Connection Manager**.
The Inventory and Connection Manager window appears.
- Step 3** From the Inventory and Connection Manager, choose **VRF management**.
The VRF Management window appears.
- Step 4** Select the VRFs you want to delete and click the **Delete** button.
The Delete VRF confirmation window appears.
- Step 5** Click **Delete** to confirm.
If the VRF objects are not in use, the selected VRF objects are deleted.

Deleting VRF Objects Associated with VRF Service Requests

A VRF object cannot be deleted if it is still associated with any VRF service request. If you attempt to do so, you receive a Delete VRF Failed message in the Status window. In this case you must first decommission, deploy, and purge all of the related VRF service requests before you can delete the VRFs object. Use the information provided in the error message to identify the VRF services requests and links related to the VRF object you are attempting to delete.

Working with VRF Service Requests

Saved VRF objects are deployed on a Provider Edge (PE) device through a special type of service request called a VRF service request. This section covers the following topics:

- [Overview of VRF Service Requests, page 3-11](#)
- [Defining VRF Service Requests, page 3-11](#)
- [Deploying VRF Service Requests, page 3-13](#)
- [Modifying VRF Service Requests, page 3-14](#)
- [Decommissioning and Deleting VRF Service Requests, page 3-14](#)
- [Searching for VRF Service Requests by VRF Object Name, page 3-15](#)
- [Viewing the Configlet Generated by a Deployed VRF Service Request, page 3-15](#)

Overview of VRF Service Requests

The VRF service request allows the VRF object to be configured on a router without having to select a physical interface. Each VRF service request consists of one or more links. Each link consists of the following elements:

- One VRF object
- One PE object
- One template (optional)

In addition, VRF service requests are associated to a customer.

**Note**

An important difference between regular MPLS service requests and VRF service requests is that there is no service policy required for a VRF service request. As a result, the VRF service request is not associated with a service policy.

The VRF service request states follow the normal ISC service request state transitions, as described in the [Service Request Transition States, page 6-1](#).

Defining VRF Service Requests

To define a VRF service request, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to access the Service Requests window.
- Step 2** Click the **Create** button and choose **VRF** from the drop-down list.
- The Service Request Editor window appears, like the one shown in [Figure 3-8](#).

Figure 3-8 Service Request Editor Window

VRF Service Request Editor

Job ID: SR ID: SR State:

Customer: Customer1

Description:

Showing 1 - 1 of 1 record

#	Link ID	VRF	PE	Template	Address Family
1.	0	Select VRF	Select PE	Select Templates	IPv4

Rows per page: 10

Go to page: 1 of 1 Go

Add Link Delete Link Save Cancel



Note If necessary, click the **Add Link** button to create a row for setting the link information.

This window allows you to define the VRF service request by setting up one or more links, each consisting of a VRF object, PE device, and an optional template. You also specify the address scheme for each link (only if the PE is running IOS XR). You can deploy any number of links with any combination of PE devices and VRF objects. An important point to note is that no physical interface on the router needs to be selected.

To set up a link, continue with the steps in the procedure, as follows:

- Step 3** Set the customer for the VRF service request by clicking on the link beside the Customer attribute. The Select Customer window appears. Choose the desired customer and click the **Select** button. This attribute is optional.
- Step 4** Click the **Select VRF** link to choose a VRF object from the ISC repository. This brings up the Select Independent VRF window, like the one shown in [Figure 3-9](#).

Figure 3-9 Select Independent VRF Window

Show VRF Objects with VRF Name matching * Find

Showing 1 - 3 of 3 records

#	VRF Name	RD Value	Provider	CERC
1.	VRF_1	100:3557	Provider1	Cerc1
2.	VRF_2	100:3000	Provider1	Cerc2
3.	VRF_3	100:3002	Provider1	Cerc1

Rows per page: 10

Go to page: 1 of 1 Go

Select Cancel

- Step 5** Choose a VRF object by clicking on a radio button and clicking the **Select** button. If desired, you can limit the VRF objects displayed by searching by VRF Name, Provider, Route Distinguisher, Route Target, or CERC using the **Show VRFs with** and **matching** fields.

**Note**

For steps on how to add VRF objects to the ISC repository, see [Creating a New VRF Object, page 3-2](#).

Step 6 Click the **Select PE** link to choose a PE device for the link.

The Select PE Device window appears.

Step 7 Choose a PE by clicking on a radio button and clicking the **Select** button.

If desired, you can limit the PE devices displayed by using the **Show PEs with** and **matching** fields.

This step specifies the PE device on which to deploy the VRF object selected in Steps 4 and 5.

**Note**

Because the VRF object and the PE device must belong to the same provider, ISC limits the list of PEs displayed to those with the same provider specified in the VRF object chosen for the link.

Step 8 Click the **Add Template** link to choose a template data file to be associated with the link.

The Add/Remove Templates window appears. This is a standard ISC window for selecting a data file and specifying operations such as append and prepend. For information on working with templates in ISC, see [Appendix B, “Working with Templates and Data Files.”](#) For specific information about using the Add/Remove Templates window, see [Using Templates and Data Files with Service Requests, page B-12](#).

Step 9 If the PE device you selected for the link is an IOS XR device, you must specify the address scheme by choosing the appropriate selection from the **Address Family** drop-down list for the link.

The choices are:

- IPv4
- IPv6
- IPv4 and IPv6

The IPv4 and IPv6 option causes the VRF object to be deployed with both IPv4 and IPv6 configurations.

**Note**

For IOS devices, the Address Family attribute defaults to IPv4. No other choice is available.

Step 10 If you want to set up additional links for the VRF service request, click the **Add Link** button and repeat Steps 4 through 9 for each link.

Step 11 When you have completed setting up the link(s) for the VRF service request, click **Save** to save the VRF service request.

The Service Requests window appears and you see the VRF service request displayed with Job ID, State, Type and other attributes. The VRF service request is initially in the Requested state.

Step 12 To deploy a VRF service request, see [Deploying VRF Service Requests, page 3-13](#).

Deploying VRF Service Requests

To deploy a VRF service request, perform the following steps.

Step 1 In the Service Requests window, choose the VRF service request you want to deploy.

- Step 2** Click the **Deploy** button and choose **Deploy** from the drop-down list.
The Deploy Service Request task window appears.
- Step 3** Set the task parameters as desired and click the **Save** button.
To immediately start the deploy task, keep the defaults and click **Save**. The Service Request window reappears and the VRF service request moves to the Deployed state.

For steps on how to check the status of the deployed VRF service request, refer to the information in [Deploying Service Requests, page 6-25](#) and [Monitoring Service Requests, page 6-27](#).

Modifying VRF Service Requests

To add links or modify existing link attributes for a VRF service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to access the Service Requests window.
- Step 2** Choose the VRF service request in the Service Requests window and click **Edit**.
The VRF Service Request Editor window appears.
- Step 3** Modify the VRF service request attributes as desired.



Note You can only modify VRF service request links that are not associated with any MPLS VPN links. When you attempt to modify any VRF service request link that is associated with an MPLS VPN link, ISC generates an error while saving the VRF service request.

- Step 4** Click **Save** to save your edits.

Decommissioning and Deleting VRF Service Requests

VRF service requests are decommissioned and deleted like other ISC service requests.



Note Decommissioning a VRF service request is not allowed if any of the links in the VRF service request with a VRF object referred in MPLS service request exists.

To decommission a VRF service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to access the Service Requests window.
- Step 2** Choose the VRF service request in the Service Requests window and click the **Decommission** button.
The Confirm Request window appears.

- Step 3** Click **OK** to confirm.
- The Service Request window appears, showing the VRF service request with a DELETE operation type.
- Step 4** Deploy the service request with the DELETE operation type, to ensure the successful decommission of the service request.
-

Searching for VRF Service Requests by VRF Object Name

To search for and display VRF service requests in the ISC repository by VRF object name, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to access the Service Requests window.
- Step 2** Choose **VRF Object Name** in the **Show Services with** drop-down list.
- Step 3** Set the **matching** and **of Type** fields as desired.
- To search only VRF service requests, choose **VRF** in the **of Type** field.
- Step 4** Click **Find** to search for service requests with the associated VRF object name you specified.
-

Viewing the Configlet Generated by a Deployed VRF Service Request

To view the configlet generated by a deployed VRF service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to view the available service requests.
- Step 2** Check the appropriate check box to select the VRF service request for which you want to view the associated configlets.
- Step 3** Click the **Details** button.
- The Service Request Details window appears.
- Step 4** Click the **Configlets** button.
- The Service Request Configlets window appears. This window displays a list of devices for which configlets have been generated.
- Step 5** To view configlets that were generated for a device, select a device and click the **View Configlet** button.
- By default, the latest generated configlet is displayed.



Note If the configlet is deployed on an IOS XR device, you have the option of displaying the configlet in XML or CLI formats or both. For more details on this behavior, see [Viewing Configlets on IOS XR Devices, page 6-32](#).

- Step 6** If applicable, you can display configlets for a device based on the time of creation. Choose the desired time of creation in the Create Time list to display a specific configlet based on the time the configlet was generated for the service request.

Step 7 Click **OK** when you are finished viewing the VRF configlet data.

Using VRFs with MPLS VPN Service Requests and Policies

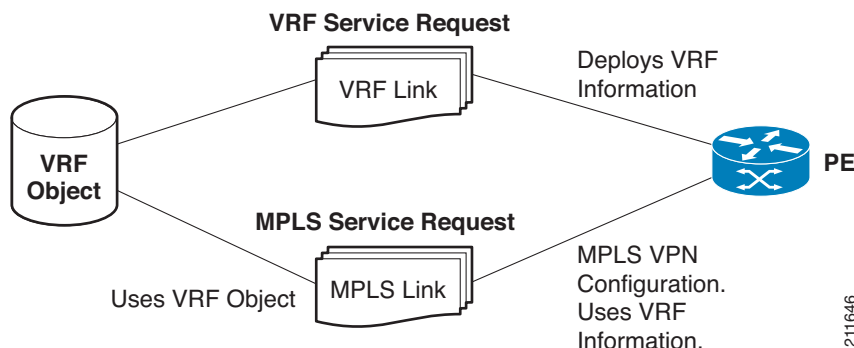
VRF objects which have been deployed can be used within MPLS VPN service requests and service policies. This section covers the following topics:

- [Relationship of VRF Object and Service Requests and PE Device, page 3-16](#)
- [Specifying VRF Objects within MPLS VPN Service Requests, page 3-16](#)
- [Searching for MPLS VPN Service Requests by VRF Object Name, page 3-20](#)
- [Searching for MPLS VPN Service Requests by VRF Object Name, page 3-20](#)
- [Specifying VRF Objects within MPLS VPN Service Policies, page 3-20](#)

Relationship of VRF Object and Service Requests and PE Device

Figure 3-10 shows the relationships between the VRF object, MPLS service request, VRF service request, and the PE device. Refer to this figure to understand concepts discussed in the procedures that follow.

Figure 3-10 VRF Object, VRF Service Request, MPLS VPN Service Request, and PE



Specifying VRF Objects within MPLS VPN Service Requests

VRF objects can be selected during the creation of the MPLS VPN service request at the time when the VRF and VPN attributes are set. At that stage, you can either set the VPN attributes individually (as in previous releases of ISC) or else use an existing VRF object. In the latter case, the MPLS VPN link “inherits” the VPN and VRF data from the VRF object. The VRF object might be either undeployed or deployed. If the VRF object is not deployed, ISC will deploy it automatically. For additional information about the function of VRF objects with MPLS VPN service requests, see [Notes On Using a VRF Object in an MPLS Service Request, page 3-20](#).

To create an MPLS VPN service request using a VRF object, perform the following steps.

- Step 1** You must create or use an existing MPLS VPN service request and follow the workflow up to the point where you define the VRF and VPN attributes. This is done in the MPLS Link Editor – VRF and VPN window, as shown in [Figure 3-11](#).

Figure 3-11 MPLS Link Attribute Editor – VRF and VPN Window

MPLS Link Attribute Editor - VRF and VPN

Attribute	Value
VRF Information	
Use VRF Object:	☐
Export Map:	
Import Map:	
Maximum Routes:	(1-4294967295)
Maximum Route Threshold *:	80 (1-100)
VRF Description:	
BGP Multipath Load Sharing:	☐
Allocate New Route Distinguisher:	☐
VRF And RD Overwrite:	☐
VPN Selection	
PE VPN Membership *:	
Select	Customer VPN Provider CERC Is Hub
Add Delete	

Note: * - Required Field



Note If necessary, see the relevant sections of this guide for how to arrive at this window in the MPLS VPN service request workflow.

- Step 2** If you do not want to use a VRF object with this MPLS VPN link, leave **Use VRF Object** unchecked. In this case, set the attributes for the VPN, as normally done with MPLS service requests. These steps are covered in other sections of this guide.
- Step 3** To use a VRF object with the MPLS VPN link, check the **Use VRF Object** check box. All of the standard VPN and VRF attributes, except BGP Multipath Load Sharing, are hidden, and the VRF Object attribute appears, as shown in [Figure 3-12](#).

Figure 3-12 MPLS Link Attribute Editor – VRF and VPN Window (Use VRF Object Selected)

Attribute	Value
VRF Information	
Use VRF Object:	☒
VRF Object *:	VRF_1 Select
BGP Multipath Load Sharing:	☐

Note: * - Required Field

- Step 4** To select a VRF object, click the **Select** button to the right of the VRF Object attribute. The Select Independent VRF window appears, as shown in [Figure 3-13](#).

Figure 3-13 Select Independent VRF Window

#	VRF Name	RD Value	Provider	CERC
1.	☐ VRF_1	100:3557	Provider1	Cerc1
2.	☐ VRF_2	100:3000	Provider1	Cerc2
3.	☐ VRF_3	100:3002	Provider1	Cerc1

Rows per page: 10 Go to page: 1 of 1 ☐ Unique RD

This Select Independent VRF window lists all of the VRF objects deployed on the PE, along with their RD value, provider and CERC information.

- Step 5** To enable the unique route distinguisher feature, check the **Unique RD** check box.



Note The Unique RD feature is restricted to one MPLS VPN link per MPLS service request. If you select the Unique RD option, it is advised that only one MPLS VPN link is present in that service request.

Be aware of the following use case scenarios when enabling the Unique RD feature:

- If the selected VRF is not deployed on any device, a VRF service request is created for the selected VRF and PE device.
- If the selected VRF is not deployed on the PE device but is deployed on a different PE device, a new VRF object is created (which is a copy of the selected VRF) and a VRF service request is created for the newly created VRF and the PE device.
- If the selected VRF is deployed only on the PE device, then nothing is done. In this case, uniqueness is automatic.
- If the selected VRF is deployed on the PE device and also on some other devices, then a new copy of the VRF object is created with an updated name and a VRF service request is created for the newly created VRF and the PE device.
- It is possible to have two VRFs with the same name but different RDs.

Step 6 Choose the desired VRF Object and click the **Select** button.



Note For information about how the selection of the VRF object is subsequently managed in ISC, see [Notes On Using a VRF Object in an MPLS Service Request, page 3-20](#), following this procedure.

Step 7 Click the **Select** button to confirm the selection of the VRF object and return to the MPLS Link Editor – VRF and VPN window.

Step 8 To set up BGP multipath load sharing, check the **BGP Multipath Load Sharing** check box. This activates additional attributes as shown in [Figure 3-14](#).

Figure 3-14 MPLS Link Attribute Editor – VRF and VPN Window (Multipath Attribute Selected)

Attribute	Value
VRF Information	
Use VRF Object:	☒
VRF Object *:	VRF_1 Select
BGP Multipath Load Sharing:	☒
BGP Multipath Action	eBGP
Force Modify Shared Multipath Attributes	☐
Maximum Paths ::	(1-32)
Import Paths:	(1-32)

Note: * - Required Field

For information on setting these attributes, see [BGP Multipath Load Sharing and Maximum Path Configuration, page 5-32](#).



Note Use the **Force Modify Shared Multipath Attributes** attribute to enable forced modification of the shared VRF attributes used by other links. This field is not persisted.

Step 9 Click the **Next** button, if you want to associate templates or data files to the service request.

The Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) When you have completed setting up templates and data files for the service request, click **Finish** in the Template Association window to close it and return to the Service Request Editor window.

Step 10 If you did not add templates, click **Finish** in the MPLS Link Editor – VRF and VPN window. The MPLS Service Request Editor window appears.

Step 11 Click the **Save** button to complete the creation of the MPLS VPN service request using the VRF object. The Service Requests window appears showing that the service request is in the Requested state and ready to deploy.

Notes On Using a VRF Object in an MPLS Service Request

Be aware of the following considerations when using VRF objects with MPLS VPN service requests:

- If the selected VRF object is not deployed on the PE device, ISC creates a new VRF service request with the selected VRF object and PE device and deploys it as part of the current MPLS VPN service request deployment process.
- If the VRF object selected in the MPLS VPN service request is not deployed on the PE device but a VRF service request exists in the Requested state or any failed states, ISC will attempt to deploy the VRF service request as part of the MPLS VPN service request.
- When decommissioning an MPLS VPN service request for which VRF service requests were created, ISC will not delete the VRF service requests automatically. The user must decommission and deploy such VRF service requests in order to delete the configuration from the device.
- When VRF configuration is selected, no VRF-related information will be provisioned on the device. The VRF name will be used in all the MPLS VPN configuration commands, such as `ip vrf forwarding` on interface, address family configuration in BGP, OSPF, EIGRP, and so on.

Searching for MPLS VPN Service Requests by VRF Object Name

To search for and display VRF service requests in the ISC repository by VRF object name, perform the following steps.

-
Step 1	Choose Service Inventory > Inventory and Connection Manager > Service Requests to access the Service Requests window.
Step 2	Choose VRF Object Name in the Show Services with drop-down list.
Step 3	Set the matching and of Type fields as desired. To search only MPLS VPN service requests, choose MPLS VPN in the of Type field.
Step 4	Click the Find button to search for MPLS VPN service requests with the associated VRF object name you specified.
-

Specifying VRF Objects within MPLS VPN Service Policies

VRF object selection is supported while defining MPLS VPN policies. This is done during the MPLS VPN policy workflow in the MPLS Policy Editor – VRF and VPN Membership window, as shown in [Figure 3-15](#).

Figure 3-15 MPLS Policy Editor – VRF and VPN Window

MPLS Policy Editor - VRF and VPN Membership

Attribute	Value	Editable			
VRF Information					
Use VRF Object:	☐	☒			
Export Map:		☒			
Import Map:		☒			
Maximum Routes:	567 (1-4294967295)	☒			
Maximum Route Threshold:	80 (1-100)	☒			
VRF Description:		☒			
BGP Multipath Load Sharing:	☐	☒			
Allocate New Route Distinguisher:	☐	☒			
VRF And RD Overwrite:	☒	☒			
VRF Name:	odVrf3	☒			
RD Value:	100:45	☒			
VPN Selection					
PE VPN Membership:		☒			
Select	Customer	VPN	Provider	CERC	Is Hub
☐	Customer1	Mpls-VPN-1	Provider1	Mpls-VPN-1	☐
Add Delete					

211712

The procedure for using the VRF Object attribute is similar to what is covered in [Specifying VRF Objects within MPLS VPN Service Requests, page 3-16](#). See that section for details on using these attributes.

If you select a VRF object for the MPLS policy, it will subsequently be used by MPLS VPN service requests that use that policy. As per standard ISC policy usage, you can check the **Editable** check box next to the VRF Object attribute to ensure that service requests based on the policy use the same VRF object specified in the policy.

**Note**

If you are not using the independent VRF object feature for the policy, then you must set the VRF and VPN attributes available in the MPLS Policy Editor – VRF and VPN Membership window. See [Defining VRF and VPN Information, page 5-29](#), for more information.

Migrating Existing MPLS VPN Service Requests to the VRF Object Model

ISC provides a migration script to migrate traditional MPLS VPN service requests to the independent VRF model. The script takes as input one or more MPLS VPN service request ID numbers and creates appropriate VRF objects and VRF service requests for each service request. The script is located in the \$ISC_HOME/bin directory. The script and its syntax is as follows:

```
runMplsSRMigration srid1 [srid2] [srid3] ...
```

Where *srid1* is the first MPLS VPN service request ID, [*srid2*] is the second service request, and so on.

ISC performs the following tasks for each MPLS VPN service request passed to the script:

- Creates a VRF object based on the VPN and VRF attributes defined for the service request.
- Copies all the VPN properties to the VRF object.
- Creates a VRF service request, with the VRF object and PE selected in the MPLS VPN link.
- Modifies the MPLS VPN link to point to the VRF object.
- Runs a configuration audit on the VRF service request and the MPLS service request to ensure the correctness of the migration.



CHAPTER 4

IPv6 and 6VPE Support in MPLS VPN

This chapter provides an overview of IPv6 and 6VPE support in MPLS VPN. It contains the following sections:

- [Overview of IPv6 and 6VPE, page 4-1](#)
- [Comparison of IOS and IOS XR, page 4-3](#)
- [ISC and MPLS VPN Updates to Support IPv6 and 6VPE, page 4-7](#)
- [IPv6 and 6VPE Features Not Supported in ISC 5.1, page 4-11](#)



Note

For information on how MPLS VPN features are implemented and supported in the ISC GUI, see the appropriate sections of this guide, as indicated by the references provided.

Overview of IPv6 and 6VPE

The ISC MPLS VPN management application supports the configuration and management of Cisco's 12000 router running IOS XR for provisioning of IPv6 VPNs and 6VPEs for ISC Layer 3 VPN services. This section provides an overview of IPv6 and 6VPE technologies. For a comparison of IOS and IOS XR, see [Comparison of IOS and IOS XR, page 4-3](#).



Note

For a list of IOS XR versions supported in ISC 5.1, see [Release Notes for Cisco IP Solution Center, 5.1](#).

Internet Protocol Version 6 (IPv6)

IPv6 is an IP protocol designed to replace IPv4, the Internet protocol that is predominantly deployed and extensively used throughout the world. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, or approximately 3.4×10^{38} addressable nodes. This provides more than enough globally unique IP addresses for every network device on the planet. Cisco Systems has added IPv6 to its Cisco IOS Software. This means that current Cisco Systems-based networks are IPv6-capable, enabling coexistence and parallel operation between IPv4 and IPv6, thereby allowing network managers to configure IPv6 when it is required. While many see IPv6 as a way to build a larger global Internet, it does not eliminate the need to create VPNs for Intranets and other similar applications.

A variety of deployment strategies are available for deploying IPv6 over MPLS backbones. Currently, service providers have two approaches to support IPv6 without making any changes to the current IPv4 MPLS backbones:

- **6PE.** Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS. 6PE lets IPv6 domains communicate with each other over an IPv4 cloud without explicit tunnel setup, requiring only one IPv4 address per IPv6 domain. The 6PE technique allows service providers to provide global IPv6 reachability over IPv4 MPLS. It allows one shared routing table for all other devices.
- **6VPE.** Cisco IPv6 VPN Provider Edge Router (6VPE) over MPLS. This facilitates the RFC 2547bis-like VPN model for IPv6 networks. 6VPE is more like a regular IPv4 MPLS VPN provider edge, with the addition of IPv6 support within Virtual Routing and Forwarding (VRF). It provides logically separate routing table entries for VPN member devices.

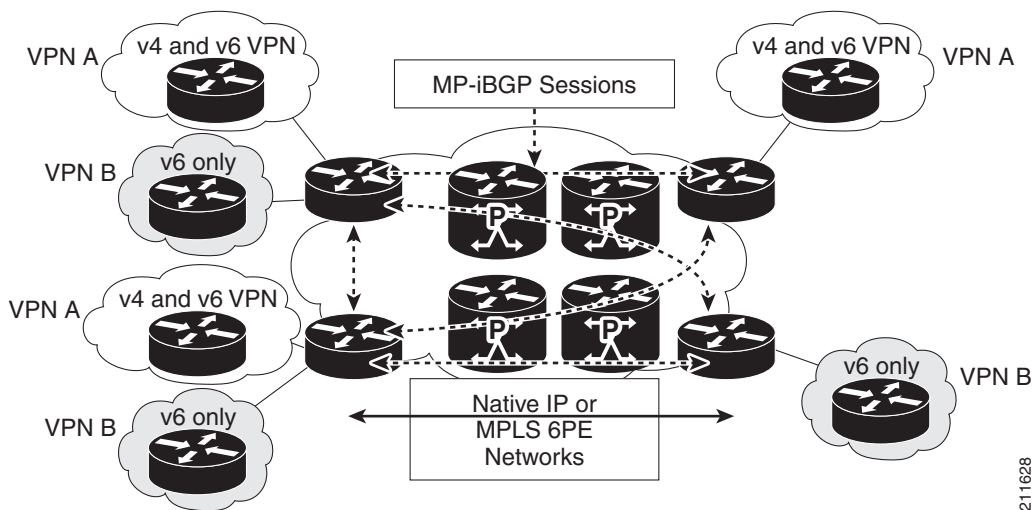
MPLS VPN in ISC 5.1 uses 6VPE to manage Layer 3 VPN services for deployment of IPv6 over a MPLS backbone.

IPv6 VPN Provider Edge Router (6VPE)

Cisco Systems's 6VPE solution smoothly introduces IPv6 VPN service in a scalable way, without any IPv6 addressing restrictions. It does not jeopardize a well-controlled service provider IPv4 backbone or any customer networks. VPN service backbone stability is a key issue for those service providers who have recently stabilized their IPv4 infrastructure. For IPv4 VPN customers, IPv6 VPN service is exactly the same as MPLS VPN for IPv4.

The IPv6 MPLS VPN service model is similar to that of IPv4 MPLS VPNs. Service providers who have already deployed MPLS IPv4 VPN services over an IPv4 backbone can deploy IPv6 MPLS VPN services over the same IPv4 backbone by upgrading the PE router IOS version and dual-stack configuration, without any change on the core routers. IPv4 services can be provided in parallel with IPv6 services. A PE-CE link can be an IPv4 link, an IPv6 link, or a combination of an IPv4 and IPv6 link, as shown in Figure 4-1.

Figure 4-1 6VPE Deployment



IPv6 VPN service is exactly the same as MPLS VPN for IPv4. 6VPE offers the same architectural features as MPLS VPN for IPv4. It offers IPv6 VPN and uses the same components, such as:

- Multiprotocol BGP (MP-BGP) VPN address family
- Route distinguishers
- VPN Routing and Forwarding (VRF) instances
- Site of Origin (SoO)
- Extended community
- MP-BGP

The 6VPE router exchanges either IPv4 or IPv6 routing information through any of the supported routing protocols, and switches IPv4 and IPv6 traffic using the respective fast switching CEF or distributed CEF path over the native IPv4 and IPv6 VRF interfaces. The 6VPE router exchanges reachability information with the other 6VPE routers in the MPLS domain using Multiprotocol BGP, and shares a common IPv4 routing protocol (such as OSPF or IS-IS) with the other P and PE devices in the domain. Separate routing tables are maintained for the IPv4 and IPv6 stacks. A hierarchy of MPLS labels is imposed on an incoming customer IPv6 packet at the edge LSR:

- Outer label (IGP Label) for iBGP next-hop, distributed by LDP.
- Inner label (VPN Label) for the IPv6 prefix, distributed by MP-BGP.

Incoming customer IPv6 packets at the 6VPE VRF interface are transparently forwarded inside the service provider's IPv4 core, based on MPLS labels. This eliminates the need to tunnel IPv6 packets. P routers inside the MPLS core are unaware that they are switching IPv6 labelled packets.

Comparison of IOS and IOS XR

This section provides a comparison between IOS and IOS XR, showing various configuration scenarios. It contains the following sections:

- [General Comparison of IOS and IOS XR Device Configlets, page 4-3](#)
- [Using OSPF as the PE-CE Routing Protocol, page 4-4](#)
- [Using EIGRP as the PE-CE Routing Protocol, page 4-5](#)
- [Using Static as the PE-CE Routing Protocol, page 4-5](#)
- [Multicast Routing on IOS XR Devices, page 4-6](#)



Note

For a list of IOS XR versions supported in ISC 5.1, see [Release Notes for Cisco IP Solution Center, 5.1](#).

General Comparison of IOS and IOS XR Device Configlets

This section provides examples of VRF-related and interface-related configlets for IOS and IOS XR.

VRF-Related Configlets

IOS

In IOS, RD and RT configlets have to be specified in IP VRF configuration mode:

```
ip vrf vrfname
  rd ASN:uniqueno
  route-target export ASN:uniqueno
  route-target import ASN:uniqueno
  route-target import ASN:uniqueno
!
```

IOS XR

In IOS XR, RT values are configured in VRF configuration mode and the RD value has to be specified under BGP configuration mode:

```
vrf vrfname
  address-family ipv4 unicast
    import route-target
      ASN:uniqueno
      ASN:uniqueno
    !
  export route-target
    ASN:uniqueno
  !
```

Router BGP mode:

```
vrf vrfname
  rd AS:uniqueno
  address-family ipv4 unicast
    redistribute connected
    redistribute static
```

Interface-Related Configlets

IOS

```
interface interfacename
ip address ipaddress subnetmask
ip vrf forwarding vrfname
```

IOS XR

```
interface interfacename
  ipv4 address ipaddress subnetmask
  vrf vrfname
```

Using OSPF as the PE-CE Routing Protocol



Note

In ISC 5.1, ISC provisions OSPF-based service requests in the same way, irrespective of whether IOS or IOS XR is used.

The following examples highlight differences between IOS and IOS XR when using OSPF as the PE-CE routing protocol.

IOS

- IOS supports the network command:

```
router ospf processid vrf vrfname
log-adjacency-changes
redistribute bgp AS subnets
network networkipadress wildcardmask area areanumber
```

- IOS supports only one VRF per OSPF process ID.

IOS XR

- In IOS XR, there is no network command support under the **ospf process id** command. In place of the network command, it uses **interface interfacename**.

```
router ospf processid
vrf vrfname
redistribute bgp AS
area areano
interface interface interfacename
```

- IOS XR supports multiple VRFs per **ospf process id** command.

```
router ospf process id
vrf vpnnew
redistribute bgp AS
area areano
interface interface interfacename
!
vrf V12:vrfname
redistribute bgp AS
area areano
interface interface interfacename
!
```

Using EIGRP as the PE-CE Routing Protocol

The following examples highlight differences between IOS and IOS XR when using EIGRP as the PE-CE routing protocol.

IOS

IOS supports multiple EIGRP process IDs per device.

IOS XR

IOS XR supports a single EIGRP process ID per device.

Using Static as the PE-CE Routing Protocol

The following examples highlight differences between IOS and IOS XR when using Static at the PE-CE routing protocol.

IOS

Configlets for creating a static route in IOS.

- When using **nexthopip** for the static route:

```
ip route vrf coke destination network subnetmask nexthopip
```

- When using **outgoing interface** for the static route

```
ip route vrf coke destination network subnetmask outgoing interface
```

IOS XR

Configlets for creating a static route in IOS XR:

- Using **outgoing interface** for the static route:

```
router static
!
vrf vrfname
  address-family ipv4 unicast
    destinationnetwork/prefixlength outgoinginterface nexthopip
  !
```

- Using **nexthopip** for the static route:

```
router static
!
vrf vrfname
  address-family ipv4 unicast
    destinationnetwork/prefixlength nexthopip
  !
```

Multicast Routing on IOS XR Devices



Note

Multicast VRF deployments for IOS XR devices are supported only for IPv4 services. Multicast cannot be enabled on IPv6 services. When multicast is enabled on IPv4+IPv6 service, only IPv4 multicast is enabled on the interface. Currently, multicast on IOS XR is supported only for IOS XR versions 3.5.2, 3.6, and 3.7.0.

This section describes how ISC supports multicast routing for IPv4 on IOS XR devices. There are no changes in the GUI (Create VPN window) to support this feature. To enable support, the IOS multicast commands are mapped to equivalent IOS XR commands. Because there are no XML configurations to support multicast routing on IOS XR devices, ISC supports the XR CLIs to enable multicast routing on IOS XR devices.

The following sections shows an example of the relevant IOS commands and the corresponding IOS XR commands to enable multicast routing.

IOS Commands

The following is a sample IOS configuration:

```
ip vrf V27:MulticastCERC3
rd 100:124
route-target import 100:406
route-target import 100:407
route-target export 100:406
mdt default 226.2.3.4
mdt data 226.5.6.7 0.0.0.15 2000
mdt mtu 2000
ip multicast-routing vrf V27:MulticastCERC3
ip pim vrf V28:VPN13 ssm default
ip pim vrf V27:MulticastCERC3 rp-address 10.20.1.1
ip pim vrf V27:MulticastCERC3 rp-address 10.20.3.1 test2
ip pim vrf V27:MulticastCERC3 rp-address 10.20.2.1 test1 override
```

IOS XR Commands

The following IOS commands are not supported on the IOS XR devices, because the corresponding commands do not exist in IOS XR.

- **ip multicast vrf <vrfName> route-limit.** The reason for not supporting this is that the command to set the route limit per VRF is not available on IOS XR devices.
- **ip pim vrf <vrfName> sparse-dense-mode.** Sparse-dense mode is not supported by IOS XR. Only sparse mode and bidirectional modes are supported.

The following IOS commands are enabled on the IOS XR device by default when the multicast routing is enabled. They cannot be disabled.

- **ip pim vrf <vrfName> sparse-mode**
- **ip pim vrf <vrfName> ssm default**
- **ip pim vrf <vrfName> autorp listener**

ISC and MPLS VPN Updates to Support IPv6 and 6VPE

This section summarizes how ISC and the MPLS VPN management application support IPv6 and 6VPE in ISC 5.1. It contains the following subsections:

- [Inventory and Device Management, page 4-7](#)
- [MPLS VPN Service Provisioning, page 4-9](#)
- [MPLS Reports, page 4-11](#)

See [Chapter 2, “Setting Up the ISC Services”](#) for information setting up ISC services mentioned in this section. For additional information on setting up basic ISC services, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

Inventory and Device Management

To activate MPLS VPN 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. Changes in this release of ISC to support inventory and device management for IPv6 and 6VPE include:

Discovery features for supporting IPv6/6VPE:

- ISC Inventory Manager supports bulk-import of 6VPE devices into the ISC repository.

Collect Config task features for supporting IPv6/6VPE:

- The Collect Config task collects device information and interface information. It has been updated to collect IPv6 addresses of interfaces. When interfaces contain both IPv4 and IPv6 addresses, both will be collected and stored in the ISC repository.
- The Collect Config task retrieves the OS type and the version information. If the device is a Cisco 12000 series router or a Cisco CRS-1 Carrier Routing System and is running IOS XR, the device will be marked as 6VPE supported.

Device configuration features for supporting IPv6/6VPE:

- 6VPE devices with IPv6 addressing can be created and managed in the ISC GUI.
 - A “6VPE” check box has been added to the Create PE Device window to designate an N-PE device as a 6VPE.
 - A new column has been added to the Interface Attributes window to show IPv6 addresses. It is not possible to bulk change the IPv6 addresses by selecting multiple interfaces. The IPv6 Address column is noneditable.
 - The Edit Device Interface window has also been updated to show IPv6 addresses on interfaces. In case of dual-stack interfaces containing both IPv4 and IPv6 addresses, both addresses are displayed.
 - The Create CPE Device window has been updated to display IPv6 addresses on interfaces. In case of dual-stack interfaces containing both IPv4 and IPv6 addresses, both addresses are displayed.
 - You cannot create an IPv6 interface using the existing Create Interface feature. This screen currently lets you create interfaces in the repository only, with the device configuration remaining unchanged. This feature does not support IPv6 addresses. The IPv6 interface creation in the device is supported through the MPLS VPN service deployment.

General features for supporting IPv6/6VPE:

- Windows within the Inventory and Connection Manager GUI have been updated in several areas to support IPv6 addressing for a 6VPE device.
- The ISC GUI provides messages to the user that IPv6 addressing scheme is only applicable to IOS XR devices.

VPN Creation and Configuration

There are no changes in the ISC VPN workflow for IPv6 and 6VPE. However, a new feature called VRF object management was added in ISC 5.0.1. See the next section, [VRF Object Support, page 4-8](#), for more information.

VRF Object Support

Starting in ISC 5.0.1, ISC allows you to specify VPN and VRF information in an independent VRF object, which is subsequently deployed to a PE device and then associated with an MPLS VPN link via an MPLS VPN service request. For details on using this feature, see [Chapter 3, “Independent VRF Management.”](#)

Resource Pools

ISC uses resource pools to automatically assign critical parameters like VLAN, VCID, and IP Addresses during the service provisioning. IPv6 address pools are not supported in this release.

MPLS VPN Service Provisioning

ISC MPLS VPN management application supports the provisioning of IPv6 Layer 3 VPNs on an IPv6 Provider Edge router (6VPE), starting with the IOS XR 3.5 release. ISC 5.1 provides the ability to configure the following on the 6VPE:

- IPv6 addressing on 6VPE (optionally, IPv4 or both IPv6+IPv4 addresses)
- Assign a static route to the 6VPE facing interface on a CE device.
- Enable MP-BGP peering with target 6VPE.
- Redistribute connected (if needed).

The following sections describe changes to MPLS VPN service policy definition, service request creation, and service request auditing to support IPv6 and 6VPE in ISC 5.1.

MPLS VPN Service Policies

Changes in this release of ISC to support MPLS VPN service policy creation for IPv6 and 6VPE include:

- The ISC MPLS VPN service policy design has been extended to support the configuration of IPv6 on a 6VPE router for the following policy types:
 - Regular: PE-CE (with unmanaged CE)
- Both Unmanaged CE and No CE scenarios are supported for IPv6.
- The service policies support the following addressing schemes:
 - IPv4
 - IPv6
 - Both IPv4 and IPv6
- The IP Numbering Scheme field in the MPLS Policy Editor - IP Address Scheme window has been updated with option to specify each of the supported address schemes.
- The IPv4 routing and IPv6 routing are independent. The ISC GUI allows you to input the same or different routing protocols for IPv4 and IPv6.
- When setting up the policy, the following PE-CE routing protocols are supported for the IPv6 addressing scheme:
 - Static
 - BGP
 - EIGRP
 - None

- IPv6 validity checks. The following checks will be performed on addresses entered in the IPv6 address fields:
 - The address can be specified eight consecutive blocks of 16-bit each separated by the “:” (colon) character. Each 16-bit block can be specified as 4-digit hexadecimal number. Example: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.
 - The leading zeros can be skipped in each hexadecimal block. Here is the modified valid address from the previous example: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.
 - Where there are consecutive “0:” blocks, they can be replaced with “::”. Example: 21DA:D3:0:0:0:FF:FE28:9C5A can be represented as 21DA:D3::FF:FE28:9C5A.
 - The string “::” cannot appear more than once in the address. Example: 21DA:0000:0000:2F3B:0000:0000:0000:9C5A can be represented as 21DA::2F3B:0000:0000:0000:9C5A or 21DA:0000:0000:2F3B::9C5A, but not as 21DA::2F3B::9C5A.

See [Chapter 5, “MPLS VPN Service Policies”](#) for information on defining MPLS VPN service policies.

MPLS VPN Service Requests

Changes for MPLS VPN policy creation to support IPv6 and 6VPE are carried over to the corresponding windows in the service request creation workflow. If the options were set as editable during policy creation, they can be modified when the service request is created.

- The IP Numbering Scheme field in the MPLS Link Attribute Editor - IP Address Scheme window has been updated with options to specify each of the supported address schemes.
- The IPv4 and IPv6 Unnumbered schemes are not supported on IOS XR devices. When you select an IOS XR device and go to the IP Addressing Scheme window, only the following options are displayed:
 - IPv4 Numbered
 - IPV6 Numbered
 - IPV4+IPV6 Numbered
- As part of the regular PE-CE MPLS service, the required VRF will be configured on the PE device. The CE-facing interface will be configured with the IPv6 address and the interface will be assigned to the VRF. The IPv6 address-family configuration in BGP along with the PE-CE routing information will be configured. The PE-CE Routing protocols supported are Static, BGP and EIGRP.
- If the PE Interface is dual-stacked and contains both IPv4 and IPv6 addresses, you can enter the routing information for both IPv4 and IPv6 independently. The GUI provides steps to enter the IPv6 routing information in addition to the existing IPv4 routing information.
- This release supports the scenario of the CE device not present in the service request. This release also supports the Unmanaged CE devices being present in the service request. In the later case, the configlets for service provisioning will be generated but not rolled onto the CE device.
- It is possible to modify a 6VPE service request.
- If the PE device is an IOS XR device, all of the configuration operations will be performed using the IOS XR interface.
- All configlets generated for 6VPE devices are IOS XR configlets and are in XML format. Different versions of IOS XR will generate different XML configlets. However, the configurations will be almost identical, except for changes in the XML schema.

See [Chapter 6, “MPLS VPN Service Requests”](#) and subsequent chapters in this guide for information on creating MPLS VPN service requests.

MPLS Service Request Audits

L3 VPN functional audit has been enhanced to support IPv6 VPNs (IPv6 addresses and 6VPE devices). The current capabilities include checking the routes to remote CEs in the VRF route tables on the PE devices. See [Auditing Service Requests, page 6-28](#) for information on auditing service requests.

MPLS Reports

The MPLS VPN reports support has been extended to support IPv6 addresses and 6VPE devices. See [Chapter 14, “Generating MPLS Reports”](#) for information on generating MPLS VPN reports for IPv6 and 6VPE.

IPv6 and 6VPE Features Not Supported in ISC 5.1

The following features are not currently supported for IPv6 and/or 6VPEs:

- Discovery of existing IPv6 VPN services on the device.
- Support of IPv6 addressing for IOS-based routers.
- IPv6 addressing as part of a CPE device definition and configuration.
- IPv6 address pools.
- IPv6 multicast address pools.
- The IPv4 and IPv6 Unnumbered address schemes are not supported for IOS XR.
- Grey management VPN support for 6VPE and IOS XR.
- Staging service request deployment to support eBGP route maps on IOS XR devices.
- Support for eBGP Extensions introduced in ISC 5.1 on IOS XR devices. These include BGP maximum path configuration, unique route distinguisher, eBGP advertisement interval, and maximum prefix configuration.
- Managed CE services.
- Multi-VRF CE (MVRFCPE) support.
- Multicast VRF for IPv6.
- One-time setup operations on the 6VPE device like enabling IPv6 routing, BGP VPNv6 configuration.
- RIP and OSPF as the PE-CE routing protocol.
- Tunnel interface. An IPv6 address cannot be specified as the Tunnel Source Address value.
- Template Manager support for IPv6 features.



CHAPTER 5

MPLS VPN Service Policies

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

- [Service Policy Overview, page 5-1](#)
- [Defining an MPLS VPN Service Policy, page 5-2](#)
- [Specifying PE and CE Interface Parameters, page 5-4](#)
- [Specifying the IP Address Scheme, page 5-8](#)
- [Specifying the Routing Protocol for a Service, page 5-11](#)
- [Defining VRF and VPN Information, page 5-29](#)
- [Enabling Template Association for a 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).

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 VPN 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.

Defining an MPLS VPN Service Policy

The remaining sections in this chapter provide an extended example of defining an MPLS service policy for a PE-CE link. This is to demonstrate the various steps involved in defining an MPLS service policy. The steps can be used as the basis for defining other types of MPLS VPN service policies. Additional types of MPLS VPN policies are described in other chapters in this guide.

To begin defining an MPLS VPN service policy for PE-CE link, perform the following steps.

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

Step 2 Choose **Policies**.

The Policies window appears.

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

The MPLS Policy Type dialog box appears, as shown in [Figure 5-1](#).

Figure 5-1 Defining the MPLS Service Policy

The screenshot shows the 'MPLS Policy Editor - Policy Type' dialog box. On the left, a sidebar indicates 'Mode: ADDING' and '1. Step 1: Policy Type'. The main area contains a table with attributes and their values:

Attribute	Value
Policy Name *	mpls_pe_ce
Policy Owner *	☒ Customer ☐ Provider ☐ Global Policy
Customer *	Select
Policy Type *	☒ Regular: PE-CE ☐ MVRFCE: PE-CE
CE Present *	☒

Step 4 Enter a **Policy Name** for the MPLS policy.**Step 5** 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.



Note For Cable (PE-NoCE), policy ownership should be set to Provider.

Step 6 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 7 Choose the **Policy Type** of the MPLS policy.

There are two policy types for MPLS policies:

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

- Step 8** Check 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 check 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 9** Click **Next**.
-

To continue with the example, see the following section, [Specifying PE and CE Interface Parameters, page 5-4](#).

Specifying PE and CE Interface Parameters

The MPLS Policy Interface dialog box appears, as shown in [Figure 5-2](#).



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 5-2 Specifying the PE UNI Security, and CE Interface Parameters

MPLS Policy Editor - Interface

Attribute	Value	Editable
Reset All Attribute Editable Flags:		☒
PE Information		
Interface Type:	ANY v	
Interface Format:		
Interface Description:		☒
Shutdown Interface:	☐	☒
Auto-Pick VLAN ID:	☐	☒
Use SVI:	☐	☒
ETTH Support:	☐	☒
Standard UNI Port:	☒	☒
UNI Security Information		
Disable CDP:	☐	☒
Filter BPDU:	☐	☒
Use Existing ACL Name:	☐	
UNI MAC Addresses:	Edit	☒
UNI Port Security:	☒	☒
Maximum MAC Address:	(1 - 5120)	☒
Aging (in minutes):	(0 - 1440)	☒
Violation Action:	PROTECT v	☒
Secure MAC Addresses:	Edit	☒
CE Information		
Interface Type:	ANY v	
Interface Format:		
Interface Description:		☒

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.

Cisco 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 check 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). Frame-Relay-ietf 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)

Table 5-1 *Interface Types and Their Corresponding Encapsulations (continued)*

Interface Type	Encapsulations (continued)
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) NOTE: [Andrew to provide content]
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) - GRE is not supported in this release. -
VLAN	None

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



Note If Auto-Pick VLAN ID is unchecked, you are prompted to enter the VLAN ID during the creation of the service request based on the policy.

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

Step 8 ETTH Support: Check this check box to configure Ethernet-To-The-Home (ETTH). For an explanation of ETTH, see [Ethernet-To-The-Home \(ETTH\)](#), page 12-9.

Step 9 Standard UNI Port: Check this check box to access UNI Security Parameters:

UNI Security Information

Step 10 Disable CDP: Check this check box to disable CDP.

Step 11 Filter BPDU: Check this check box to filter BPDU.

Step 12 Use existing ACL Name: Check this check box to use existing ACL name.

Step 13 UNI MAC Addresses: Click **Edit** to modify or create a MAC address record.

Step 14 UNI Port Security: Check this check box to access UNI Port Security parameters:

- a. **Maximum MAC Address:** Enter a valid value.
- b. **Aging (in minutes):** Enter a valid value.

- c. **Violation Action:** From the drop-down list, choose one of the following:
 - PROTECT
 - RESTRICT
 - SHUTDOWN
- d. **Secure MAC Address:** Click **Edit** to modify or create a secure MAC address record.

CE Interface Information

- Step 15 Interface Type:** From the drop-down list, choose the interface type for the CE.
- Step 16 Interface Format:** Optionally, you can specify the slot number and port number for the CE interface.
- Step 17 Interface Description:** Optionally, you can enter a description of the CE interface.
- Step 18 Encapsulation:** Choose the encapsulation used for the specified CE interface type.
- Step 19** When satisfied with the interface settings, click **Next**.

To continue with the example, see the following section, [Specifying the IP Address Scheme, page 5-8](#).

Specifying the IP Address Scheme

The MPLS Policy Interface Address Selection window appears, as shown in [Figure 5-3](#).

Figure 5-3 Specifying the IP Address Scheme

Attribute	Value	Editable
PE-MVRFC Interface Address/Mask		
IP Numbering Scheme:	IPv4 Numbered	☒
Extra MVRFC Loopback Required:	☐	☒
Automatically Assign IP Addresses:	☒	☒
IP Address Pool:	Region Pool	☒

To specify the IP address scheme you want to use for this service policy, perform the following steps.

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

IP Numbering Scheme

You can choose from the following options.

- **IPv4 Numbered**

If you choose **IPv4 Numbered** and also check 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 IPv4 addresses from a /30 subnet point-to-point IP address pool.

- **IPv4 Unnumbered**

IPv4 addresses are drawn from the loopback IPv4 address pool. An unnumbered IPv4 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 **IPv4 Unnumbered**, ISC: MPLS creates a static route for the PE-CE link.

When you choose **IPv4 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 5-10](#).

- **IPv6 Numbered**

This addressing scheme is provided to support a 6VPE router. See [Chapter 4, “IPv6 and 6VPE Support in MPLS VPN”](#) for more information on IPv6 and 6VPE support in MPLS VPN management.



Note This option only appears if the policy type is a regular PE-CE policy.

- **IPv4+IPv6 Numbered**

In the case of a 6VPE device, the PE interface can be “dual stacked,” meaning it can contain both IPv4 and IPv6 addresses. In later steps, you will be able to enter the routing information independently for both IPv4 and IPv6. See [Chapter 4, “IPv6 and 6VPE Support in MPLS VPN”](#) for more information on IPv6 and 6VPE support in MPLS VPN management.



Note This option only appears if the policy type is a regular PE-CE policy.

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 **IPv4 Unnumbered** and also check 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 **IPv4 Numbered** and also check 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.



Note This option is not supported for the **IPv6 Numbered** and **IPv4+IPv6 Numbered** address schemes.

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.



Note This option is not supported for the IPv6 Numbered and IPv4+IPv6 Numbered address schemes.

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.

To continue with the example, see the following section, [Specifying the Routing Protocol for a Service, page 5-11](#).

Specifying the Routing Protocol for a Service

You can now specify the routing protocol information for this service policy, as shown in [Figure 5-4](#).

**Note**

IPv4 and IPv6 routing are independent. The ISC GUI allows you to input the same or different routing protocols for IPv4 and IPv6, depending upon which addressing scheme you selected. Not all routing protocols are supported for IPv6. See [Chapter 4, “IPv6 and 6VPE Support in MPLS VPN”](#) for more information IPv6 and supported routing protocols.

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 5-12](#)).
- **RIP**—Routing Information Protocol (see [RIP Protocol Chosen, page 5-14](#)).
- **BGP**—Border Gateway Protocol (see [BGP Protocol Chosen, page 5-18](#)).
- **OSPF**—Open Shortest Path First (see [OSPF Protocol Chosen, page 5-21](#)).
- **EIGRP**—Enhanced Interior Gateway Routing Protocol (see [EIGRP Protocol Chosen, page 5-24](#)).
- **None**. Specifies parameters for cable services (see [None Chosen: Cable Services, page 5-28](#)).

To specify a routing protocol for the PE-CE link, perform the following steps.

Step 1 Choose the appropriate protocol from the Routing Protocol drop-down list.

**Note**

For IPv6, only Static, BGP, EIGRP and None are supported and are available in the drop-down list.

When you choose a particular routing protocol, the related parameters for that protocol are displayed.

Step 2 Enter the required information for the selected routing protocol, then click **Next**.

Step 3 Define the MPLS Policy VRF and VPN Selection parameters as described in [Defining VRF and VPN Information, page 5-29](#).

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 might 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)**, as shown in [Figure 5-4](#).

**Note**

Two other options (**AdvertisedRoutes** and **Default Routes - Routes to reach other sites**) are available when you create the service request. See [Setting Static Routing Protocol Attributes \(for IPv4 and IPv6\)](#), page 6-13.

Figure 5-4 Specifying the Static Routing Protocol

Attribute	Value	Editable
PE-CE Ipv4 Routing Information		
Routing Protocol	STATIC	☒
CsC Support:	☐	☒
Give Only Default Routes to CE:	☐	☒
Redistribute Connected (BGP only):	☐	☒
Default Information Originate (BGP only):	☐	☒

To specify Static as the routing protocol for the service policy, perform the following steps.

- 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 VRF and VPN Information](#), page 5-29.

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.

To specify RIP as the routing protocol for the service policy, perform the following steps.

Step 1 Choose **RIP** from the Routing Protocol drop-down list.

The RIP Routing Protocol dialog box appears, as shown in [Figure 5-5](#).

Figure 5-5 RIP Selected as the Routing Protocol

Attribute	Value	Editable
PE-CE IPv4 Routing Information		
Routing Protocol	RIP	☒
CsC Support:	☒	☒
Give Only Default Routes to CE:	☒	☒
Redistribute Static (BGP only):	☒	☒
Redistribute Connected (BGP only):	☒	☒
RIP Metrics (BGP only):	(1-16)	☒
Redistributed Protocols on PE:	Edit	☒
Redistributed Protocols on CE:	Edit	☒

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 PE Redistributed Protocols dialog box appears.

- 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

- d. Choose the protocol you want to redistribute into RIP 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 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:

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

The CE Redistributed Protocol dialog box appears.

- b. Click **Add**.

The CE Redistributed Protocols dialog box appears.

- 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**, **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, ISC 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

- d. Choose the protocol you want to redistribute into RIP 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 RIP on the CE, then click **OK**.

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

The MPLS Policy VRF and VPN Membership dialog box appears. To proceed, see [Defining VRF and VPN Information, page 5-29](#).



Note

If a PE link is initially configured to use the RIP routing protocol and subsequently modified to use another routing protocol (or static routing), ISC does not remove all of the RIP CLI commands associated with the interface from the PE configuration file. Specifically, ISC does not remove the address family subcommands under the RIP command unless the VRF associated with the service request is removed. This is because ISC configures the RIP protocol using a network class (that is, network a.0.0.0) based under address-family. Later, if the routing protocol is changed, ISC does not remove any other services under the same network.

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.

To specify BGP as the routing protocol for the service policy, perform the following steps.

Step 1 Choose **BGP** from the Routing Protocol drop-down list.

The BGP Routing Protocol dialog box appears, as shown in [Figure 5-6](#).

Figure 5-6 BGP Selected as the Routing Protocol

Attribute	Value	Editable
PE-CE Ipv4 Routing Information		
Routing Protocol	BGP	✓
CsC Support:	☒	✓
Redistribute Static (BGP only):	☒	✓
Redistribute Connected (BGP only):	☒	✓
CE BGP AS ID:	(1-65535)	✓
Neighbor Allow-AS in:	(1-10)	✓
Neighbor AS Override:	☐	✓
Redistributed Protocols on CE:	Edit	✓
Advertise Interval:	(1-600 Seconds)	✓
Max Prefix Number:	(1-2147483647)	✓
Max Prefix Threshold:	(1-100 %)	✓
Max Prefix Warning Only:	☐	✓
Max Prefix Restart:	(1-65535 Minutes)	✓

Step 2 CSC Support: To define a Service Policy with Carrier Supporting Carrier (CSC), check 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) Indicate whether you want to redistribute static routes into BGP.

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

Step 4 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 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 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 6 Neighbor Allow-AS In: If appropriate, enter the **Neighbor Allow-AS-in** value.

When you enter a **Neighbor Allow-AS-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 7 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 8 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 CE Redistributed Protocols dialog box appears.

- 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 (Routing Information 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 do not 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** 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 9 Advertise Interval: Enter the eBGP advertisement interval.

The value is an integer ranging from 0 to 600, specifying the number of seconds of the advertisement interval. The default setting is 30 seconds for the eBGP peer, if it is not explicitly configured.

Step 10 Max Prefix Number: Enter the maximum number of prefixes that can be received from a neighbor.

The range is 1 to 2147483647. This feature allows a router to bring down a peer when the number of received prefixes from that peer exceeds the limit.

Step 11 Max Prefix Threshold: Enter a value that specifies at what percentage Max Prefix Number is configured.

The range is from 1 to 100 percent, with the default being 75 percent. When this threshold is reached, the router generates a warning message. For example, if the Max Prefix Number is 20 and the Max Prefix Threshold is 60, the router generates warning messages when the number of BGP learned routes from the neighbor exceeds 60 percent of 20, or 12 routes.

Step 12 Max Prefix Warning Only: Check this check box if you want to allow the router to generate a log message when the maximum prefix limit is exceeded, instead of terminating the peering session.

Step 13 Max Prefix Restart: Enter a value, in minutes, specifying when the router will automatically re-establish a peering session that has been brought down because the configured maximum prefix limit has been exceeded.

The range is from 1 to 65535. No intervention from the network operator is required when this feature is enabled. This feature attempts to re-establish a disabled peering session at the configured time interval that is specified. However, the configuration of the restart timer alone cannot change or correct a peer that is sending an excessive number of prefixes. The network operator will need to reconfigure the maximum prefix limit or reduce the number of prefixes that are sent from the peer. A peer that is configured to send too many prefixes can cause instability in the network, where an excessive number of prefixes are rapidly advertised and withdrawn. In this case, the Max Prefix Warning Only attribute can be configured to disable the restart capability, while the network operator corrects the underlying problem.

Step 14 When you are satisfied with the BGP protocol settings for this service policy, click **Next**.

The MPLS Policy VRF and VPN Membership dialog box appears. To proceed, see [Defining VRF and VPN Information](#), page 5-29.

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.

To specify OSPF as the routing protocol for the service policy, perform the following steps.

Step 1 Choose **OSPF** from the Routing Protocol drop-down list.

The OSPF Routing Protocol dialog box appears, as shown in [Figure 5-7](#).

Figure 5-7 OSPF Selected as the Routing Protocol

Attribute	Value	Editable
PE-CE Ipv4 Routing Information		
Routing Protocol	OSPF	☒
CsC Support:	☐	☒
Metric to Redistribute OSPF into iBGP:	(0-4294967295)	☒
Give Only Default Routes to CE:	☐	☒
Redistribute Static (BGP only):	☐	☒
Redistribute Connected (BGP only):	☐	☒
OSPF Process ID on PE:	(1-65535)	☒
OSPF Process ID on CE:	(1-65535)	☒
OSPF Area Number or IP Address:	(0 - 4294967295 or a.b.c.d)	☒
Redistributed Protocols on PE:	Edit	☒
Redistributed Protocols on CE:	Edit	☒

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, check 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 PE Redistributed Protocols dialog box appears.

- 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 CE Redistributed Protocols dialog box appears.

- 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 are satisfied with the OSPF protocol settings for this service policy, click **Next**.

The MPLS Policy VRF and VPN Membership dialog box appears. To proceed, see [Defining VRF and VPN Information, page 5-29](#).

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 autosummarizes 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.

To specify EIGRP as the routing protocol for the service policy, perform the following steps.

Step 1 Choose **EIGRP** from the Routing Protocol drop-down list.

The EIGRP Routing Protocol dialog box appears, as shown in [Figure 5-8](#).

Figure 5-8 EIGRP Selected as the Routing Protocol

MPLS Policy Editor - Ipv4 Routing Information

Attribute	Value	Editable
PE-CE Ipv4 Routing Information		
Routing Protocol	EIGRP	☒
CsC Support:	☐	☒
Redistribute Static (BGP only):	☐	☒
Redistribute Connected (BGP only):	☐	☒
EIGRP AS ID on PE:	(1-65535)	☒
EIGRP AS ID on CE:	(1-65535)	☒
Bandwidth Metric:	(1-4294967295)	☒
Delay Metric:	(1-4294967295)	☒
Reliability Metric:	(0-255)	☒
Loading Metric:	(1-255)	☒
MTU Metric:	(1-4294967295)	☒
Redistributed Protocols on PE:	Edit	☒
Redistributed Protocols on CE:	Edit	☒

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 PCP 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 autosummarizes 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 PE Redistributed Protocols dialog box appears.

- 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 CE Redistributed Protocols dialog box appears.

- 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

- Choose the protocol you want to redistribute into EIGRP 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 EIGRP on the CE, then click **OK**.

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

The MPLS Policy VRF and VPN Membership dialog box appears. To proceed, see [Defining VRF and VPN Information](#), page 5-29.

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.

If this service policy is for cable services, perform the following steps.

Step 1 Choose **None** from the list of routing protocols.

The following dialog box appears, as shown in [Figure 5-9](#).

Figure 5-9 No Routing Protocol Selected

Attribute	Value	Editable
PE-CE IPv4 Routing Information		
Routing Protocol	NONE	☒
CsC Support:	☒	☒
Redistribute Static (BGP only):	☒	☒
Redistribute Connected (BGP only):	☒	☒

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**.

The MPLS Policy VRF and VPN Membership dialog box appears. To proceed, see [Defining VRF and VPN Information](#), page 5-29.

Defining VRF and VPN Information

When you are finished defining the routing protocol(s) for the service policy, you must then specify the VRF and VPN information for this service policy. To do this, perform the following steps.

- Step 1** The MPLS Policy VRF and VPN Membership dialog box appears, as shown in [Figure 5-10](#).

Figure 5-10 Specifying the VRF Information

Attribute	Value	Editable
VRF Information		
Use VRF Object:	☐	☒
Export Map:		☒
Import Map:		☒
Maximum Routes:	(1-4294967295)	☒
Maximum Route Threshold:	80 (1-100)	☒
VRF Description:		☒
BGP Multipath Load Sharing:	☐	☒
Allocate New Route Distinguisher:	☐	☒
VRF And RD Overwrite:	☐	☒
VPN Selection		
PE VPN Membership:	☐	☒

Select Customer VPN Provider CERC Is Hub

Add Delete

- Step 2** If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box.

For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

If you are not using the VRF object feature, then define the VRF and VPN attributes as described in the following steps.

Step 3 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 4 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 5 Maximum Routes: Specify the maximum number of routes that can be imported into the VRF on this PE.**Note**

ISC will not allow provisioning of another value for Maximum Routes after it is configured with a value. Because a VRF might be used by multiple interfaces (links), after this value is configured for a link, it is recommended that you do not manually change it. ISC generates an error if you try to change the maximum routes value for an existing or new service request using this VRF.

Step 6 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 7 VRF Description: Optionally, you can enter a description of the VRF for the current VPN.**Step 8 BGP Multipath Load Sharing:** Check this check box to enable BGP multipath load sharing and maximum path configuration.

See [BGP Multipath Load Sharing and Maximum Path Configuration, page 5-32](#), for details on using this option.

Step 9 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, reuse 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 is not found on the PE, create it.



Note The service request 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.



Note The **Allocate New Route Distinguisher** option is disabled if you enabled the unique route distinguisher feature when the VPN was created. For information, see [Enabling a Unique Route Distinguisher for a VPN, page 2-28](#).

Step 10 VRF and RD Overwrite: When you enable the **VRF and RD Overwrite** option, this dialog box presents two new fields, as shown in [Figure 5-11](#), 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.



Note The **VRF and RD Overwrite** option is disabled if you enabled the unique route distinguisher feature when the VPN was created. For information, see [Enabling a Unique Route Distinguisher for a VPN, page 2-28](#).

Figure 5-11 No Routing Protocol Selected

VRF And RD Overwrite	☒	☒
VRF Name:		☒
RD Value:		☒

89754

a. **VRF Name:** Enter the new VRF name. It is recommended not to use special characters (' ` " < > () [] { } / \ & ^ ! ? ~ * % = , . + |), as this may cause misconfiguration of the VRF name for certain devices.

b. **RD Value:** Enter the new RD value.

Step 11 PE VPN Membership: In the 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 12 If you would like to enable template and data file support for the policy, click the **Next** button to access the Template Association window, and then refer to [Enabling Template Association for a Policy, page 5-34](#) details on working with templates and data files.

Step 13 If you are satisfied with the VRF and VPN selections, click **Finish**.

The Policies window appears.

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.”](#)

BGP Multipath Load Sharing and Maximum Path Configuration

ISC supports the configuration of Border Gateway Protocol (BGP) multipath load sharing for external BGP (eBGP), internal BGP (iBGP), and external and internal BGP (eiBGP). As additional support for BGP multipath load sharing, MPLS also allows setting a unique route distinguisher (RD) per provider edge (PE) router for a virtual private network (VPN) and virtual route forwarding (VRF) table. The **BGP Multipath Load Sharing** option allows you to enable or disable BGP multipath load sharing, as shown in [Figure 5-12](#).

Figure 5-12 Multipath Configuration Options of the VRF and VPN Membership Window

BGP Multipath Load Sharing:	☒	☒
BGP Multipath Action	iBGP	☐
Maximum Paths ¹ :	(1-32)	☐
Import Paths:	(1-32)	☐
Unequal Cost:	☐	☒

When the **BGP Multipath Load Sharing** check box is checked, additional fields are displayed for the BGP multipath action, maximum paths, import paths, and unequal cost routes.



Note

The additional fields appear dynamically in the GUI based on the **BGP Multipath Action** option you choose.

If there is no existing BGP multipath configuration, specifying multipath load sharing through these fields creates a new multipath BGP configuration for the VRF of the PE. If a BGP multipath configuration already exists, this action overwrites the existing configuration with the new multipath values. A remove option allows you to delete all existing BGP multipath configurations of a particular type for the VRF of the PE. If the **BGP Multipath Load Sharing** check box is unchecked, no BGP multipath actions are taken. See [Removing a Multipath Configuration, page 5-34](#), for how multipath settings defined in a service request can be removed.

The following sections describe each of the multipath scenarios, as determined by the type of BGP multipath selected in the **BGP Multipath Action** drop-down list. The options available in the drop-down list are:

- **eBGP**—Specifies the multipath configuration for eBGP. This is the default selection.
- **iBGP**—Specifies the multipath configuration for iBGP.
- **eiBGP**—Specifies the multipath configuration for both eBGP and iBGP. This option allows you to set a common shared value for maximum paths and import paths for both eBGP and iBGP.

- **eBGP+iBGP**—Specifies the multipath configuration for both eBGP and iBGP. This option allows you to set the maximum paths and import paths separately for both eBGP and iBGP.
- **Remove**—Deletes all existing BGP multipath configurations for the VRF of the PE.

Each of these scenarios is covered below.



Note

When creating service requests, in the MPLS Link Editor - VPN and VRF window, an additional BGP attribute called **Force Modify Shared Multipath Attributes** appears in the GUI when the **BGP Multipath Load Sharing** check box is checked. The purpose of this attribute is to enable forced modification of the shared VRF attributes used by other links. This field is not persisted. This attribute only appears when creating service requests, not when creating policies.

eBGP Multipath

When you select the **eBGP** option, the **Maximum Paths** and **Import Paths** fields appear. Where:

- **Maximum Paths**—Specifies the maximum number of routes to allow in the routing table.
- **Import Paths**—Specifies the number of redundant paths that can be configured as backup multipaths for a VRF.



Note

When setting up an eBGP multipath configuration, you must set a value for either **Maximum Paths** or **Import Paths**. Both fields cannot be blank.

iBGP Multipath

When you select the **iBGP** option, the **Maximum Paths**, **Import Paths**, and **Unequal Cost** fields appear. Where:

- **Maximum Paths**—Specifies the maximum number of routes to allow in the routing table. You must specify a value when setting up an iBGP multipath configuration.
- **Import Paths**—Specifies the number of redundant paths that can be configured as backup multipaths for a VRF.
- **Unequal Cost**—Enables/disables unequal-cost multipath. Unequal-cost multipath allows traffic to be distributed among multiple unequal-cost paths to provide greater overall throughput and reliability.

eiBGP Multipath

When you select the **eiBGP** option, the **Maximum Paths** and **Import Paths** fields appear. Where:

- **Maximum Paths**—Specifies the maximum number of routes to allow in the routing table. You must specify a value when setting up an eiBGP multipath configuration.
- **Import Paths**—Specifies the number of redundant paths that can be configured as backup multipaths for a VRF.

eiBGP+iBGP Multipath

When you select the **eiBGP+iBGP** option, the **Maximum Paths**, **Import Paths**, and **Unequal Cost** fields appear. Where:

- **Maximum Paths**—Specifies the maximum number of routes to allow in the routing table. The number of routes can be specified separately for eBGP and iBGP.
- **Import Paths**—Specifies the number of redundant paths that can be configured as backup multipaths for a VRF. The number of paths can be specified separately for eBGP and iBGP.

- **Unequal Cost**—Enables/disables unequal-cost multipath. Unequal-cost multipath allows traffic to be distributed among multiple unequal-cost paths to provide greater overall throughput and reliability.

**Note**

The support for multipath load sharing requires unique route distinguishers (RDs) for each PE router for a VPN (VRF). This is to prevent the same RDs from being allocated to different customers. This allows the use of the same RD for the same VRF. That is, all sites in the PE can have the same unique RD. The unique RD feature is optional. It is enabled at both a global VPN level or a service request level. To enable the unique RD per PE for a VPN, the Create VPN window contains a new **Enable Unique Route Distinguisher** field. For more information on using this feature, see [Enabling a Unique Route Distinguisher for a VPN, page 2-28](#).

Removing a Multipath Configuration

A multipath configuration can be removed by selecting the **Remove** option in drop-down list of the BGP Multipath Action attribute. The Remove option removes the multipath configuration for the VRF on the PE, if it is previously configured.

If a service request is saved with a multipath configuration and the configuration has to be removed, you should use the Remove option.

**Note**

A multipath configuration cannot be removed by simply unchecking the BGP Multipath Load Sharing check box. It must be removed by setting the BGP Multipath Action attribute to Remove, and then saving the service request. You should uncheck the BGP Multipath Load Sharing check box only after removing the multipath configuration.

Enabling Template Association for a Policy

The ISC template feature gives you a means to download free-format CLIs to devices configured for links within an MPLS service request. If you enable templates, you can use templates and data files to download commands that are not currently supported by ISC.

- Step 1** To enable template association for the policy, click the **Next** button in MPLS Policy Editor - VRF and VPN Membership window.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) For additional information about using templates in ISC, also see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

- Step 2** When you have completed setting up templates and data files for the policy per the instructions in the appendix, click **Finish** in the Template Association window to close it.

The Policies window appears.

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.”](#)



CHAPTER 6

MPLS VPN Service Requests

This chapter describes how to provision and audit service requests in IP Solution Center (ISC). It contains the following major sections:

- [Overview of Service Requests, page 6-1](#)
- [Examples of Creating MPLS VPN Service Requests, page 6-6](#)
- [Deploying Service Requests, page 6-25](#)
- [Monitoring Service Requests, page 6-27](#)
- [Auditing Service Requests, page 6-28](#)
- [Viewing Configlets Generated by a Service Request, page 6-31](#)
- [Editing Configuration Files, page 6-33](#)

Overview of Service Requests

This section contains the following sections:

- [Service Request Transition States, page 6-1](#)
- [Service Enhancements, page 6-5](#)
- [How ISC Accesses Network Devices, page 6-5](#)
- [MPLS VPN Topology Example, page 6-6](#)

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.

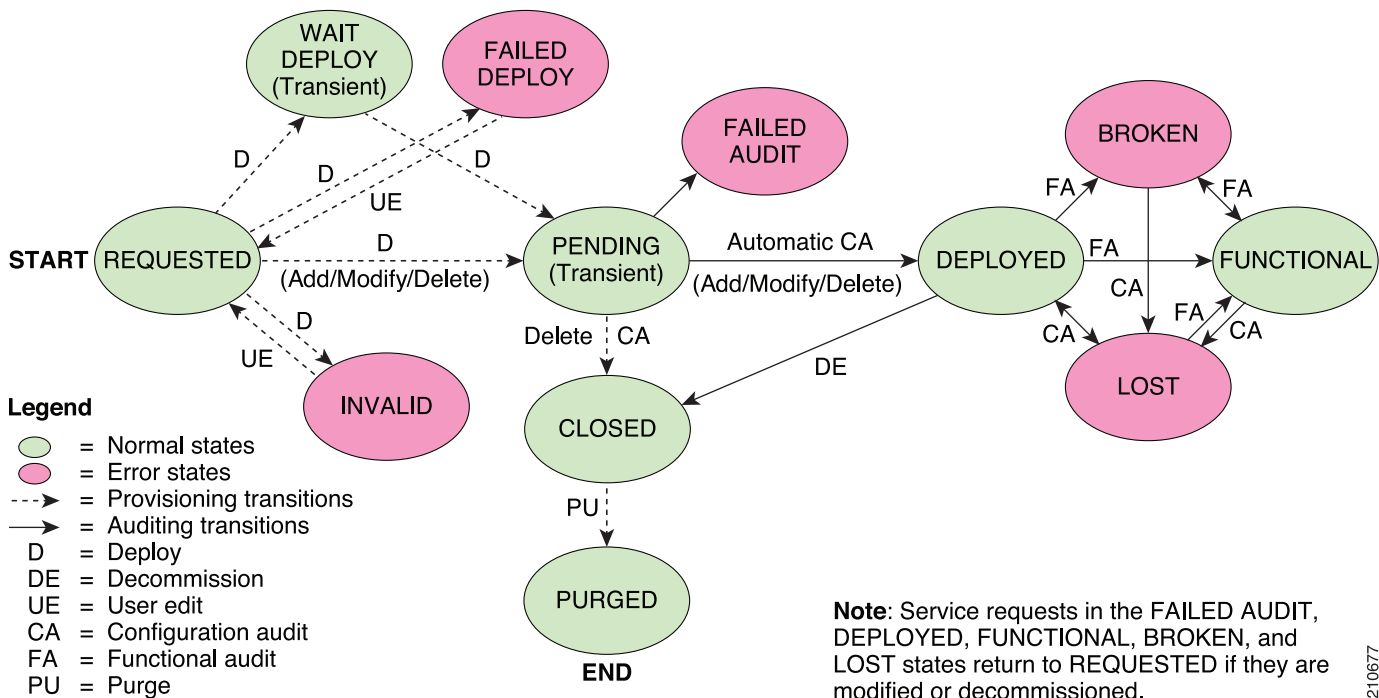
ISC steps the operator through the process and simplifies the task of provisioning the CE and PE by automating most of the tasks required to set up an MPLS VPN.

Figure 6-1, “Service Requests States Transition Diagram,” 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 D, “Service Request Transition States.”

**Note**

ISC service requests are processed in parallel, except when multiple service requests attempt to configure the same device. In this case, the service requests are processed sequentially (that is, only one write to the device can happen at a time).

Figure 6-1 Service Requests States Transition Diagram



210677

Table 6-1, “Summary of Cisco IP Solution Center Service Request States,” describes the functions of each ISC service request state. They are listed in alphabetic order.

Table 6-1 Summary of Cisco IP Solution Center Service Request States

Service Request Type	Description
Broken (valid only for MPLS services)	The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example). An MPLS service request moves to Broken if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent.
Closed	A service request moves to Closed if the service request should no longer be used during the provisioning or auditing process. A service request moves to the Closed state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.
Deployed	A service request moves to Deployed if the intention of the service request is found in the router configuration file. Deployed indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
Failed Audit	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the Deployed state. The Failed Audit state is initiated from the Pending state. After a service request is deployed successfully, it cannot re-enter the Failed Audit state (except if the service request is redeployed).
Failed Deploy	The cause for a Failed Deploy status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
Functional (valid only for MPLS services)	An MPLS service request moves to Functional when the auditor finds the VPN routing and forwarding tables (VRF) for this service and they match with the service intent. This state requires that both the configuration file audit and the routing audit are successful.
Invalid	Invalid indicates that the service request information is incorrect in some way. A service request moves to Invalid if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to Lost when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the Deployed state, but now some or all router configuration information is missing. A service request can move to the Lost state <i>only</i> when the service request had been Deployed .

Table 6-1 Summary of Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
Pending	A service request moves to Pending when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. Pending indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers. The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is performed and the service is still pending, it is in an error state.
Requested	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains Requested, the service is in an error state.
Wait Deploy	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. Wait Deploy indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the Wait Deploy state are then downloaded to the Cisco CNS-CE server.

Table 6-2, “User Operations on ISC Service Requests,” describes user operations and their impact on ISC service requests.

Table 6-2 User Operations on ISC Service Requests

User Operations	Description
Decommission	This user operation removes the service from all devices in the service request.
Force Deploy	This user operation allows you to Deploy a service request from any state except Closed . This is equivalent to restarting the state diagram. The service request can move from its current state to any other possible state. However, it does not move to the Requested state.
Force Purge	This user operation removes a service request from the database irrespective of its state. If you Force Purge a service request from the ISC repository before first decommissioning the service request, the service remains running on the network (specifically, the configuration remains on the devices on which the service was provisioned), but all record of the service request that created the service is removed from ISC.
Purged	When a service request is Purged , it is removed from the ISC database.

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 (host name 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.

Examples of Creating MPLS VPN 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 5, “MPLS VPN Service Policies.”](#)

This section covers the following topics:

- [MPLS VPN Topology Example, page 6-6](#)
- [Creating an MPLS VPN PE-CE Service Request, page 6-7](#)
- [Creating a Multi-VRF Service Request, page 6-15](#)
- [Creating a PE-Only Service Request, page 6-20](#)

**Note**

Subsequent chapters in this guide provide additional examples of setting up these and other MPLS VPN service requests. See also [Chapter 7, “Provisioning Regular PE-CE Links”](#) and [Chapter 8, “Provisioning Multi-VRFCE PE-CE Links.”](#)

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).

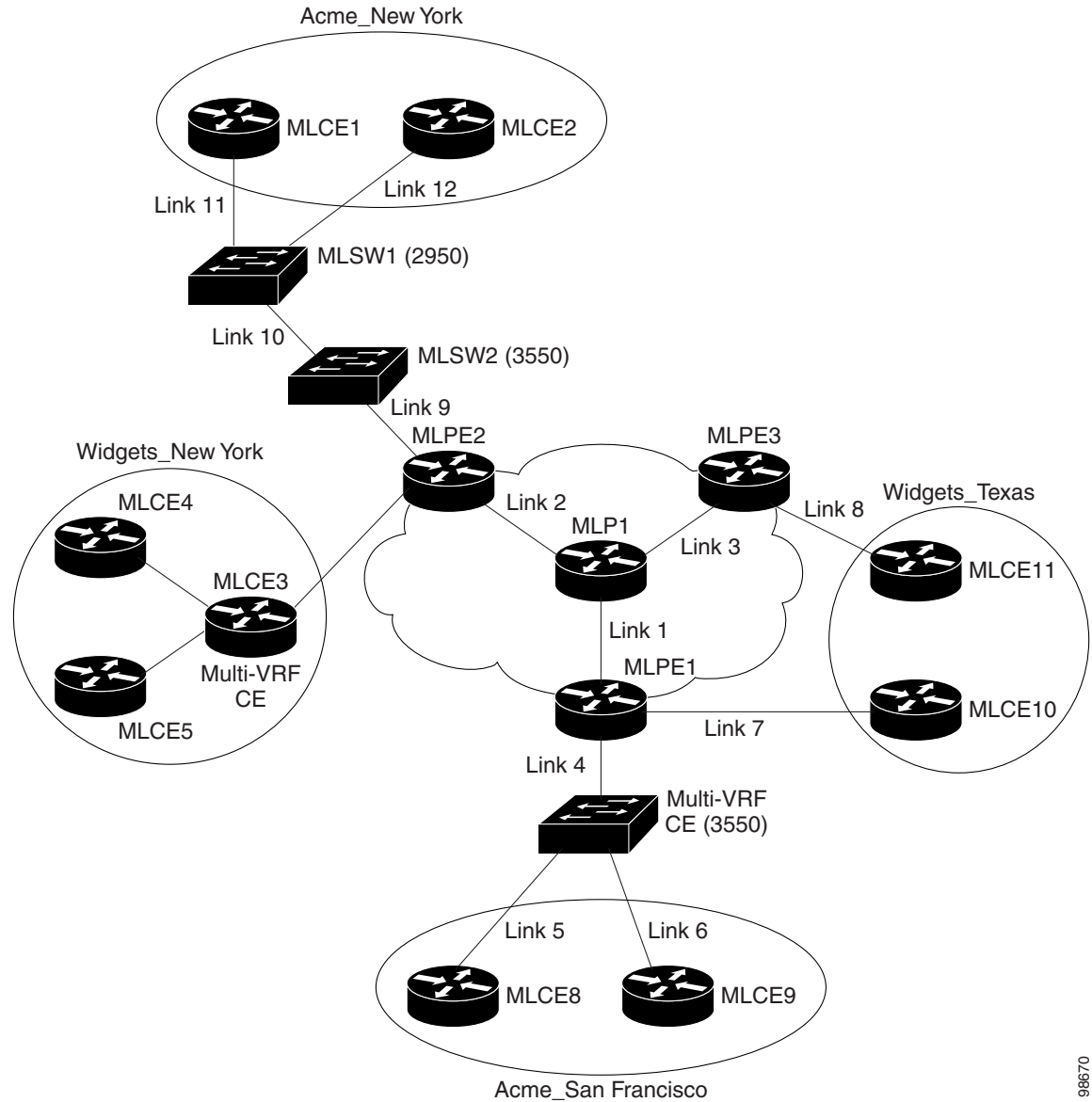
Multi-VRF Example

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 an MPLS VPN PE-CE Service Request

For an example of creating an MPLS VPN PE-CE service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.
The Service Requests dialog box appears.

- Step 2** To start the process to create a new service, click **Create**.
A drop-down list appears, showing the types of service requests you can create.
- Step 3** Choose **MPLS VPN**.
The Select MPLS Policy dialog box appears. It displays the list of all the MPLS service policies that have been defined in ISC.
- Step 4** Choose the policy of choice, then click **OK**.
The MPLS Service Request Editor appears.
- Step 5** Click **Add Link**.
The MPLS Service Request Editor now displays a set of fields, as shown in [Figure 6-3](#). 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 6-3 Initial Fields Displayed to Define PE-CE Link

Showing 1-1 of 1 records								
#	☐	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	☐	0	Select CE		Select PE		Add	N/A

- Step 6** CE: Click **Select CE**.
The Select CPE Device dialog box appears, as shown in [Figure 6-4](#).

Figure 6-4 Selecting the CE for the MPLS Link

Select CPE Device - Microsoft Internet Explorer

CPE for MPLS VPN Link

Show CPEs with matching

Showing 1-5 of 12 records

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	☒	mlce1.cisco.com	AcmeInc	Acme_NY	MANAGED
2.	☐	mlce2.cisco.com	AcmeInc	Acme_NY	MANAGED
3.	☐	mlce8.cisco.com	AcmeInc	Acme_SF	MANAGED_MGMT_LAN
4.	☐	mlce9.cisco.com	AcmeInc	Acme_SF	MANAGED
5.	☐	mlce12.cisco.com	AcmeInc	Acme_TX	MANAGED

Rows per page: << Page 1, 2, 3 >>

- 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**.

- d. 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, as shown in [Figure 6-5](#).

Figure 6-5 CE and CE Interface Fields Defined

Showing 1-1 of 1 records								
#	☐	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	☐	0	mlce1	FastEthernet0/1	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 appears.

- a. From the “Show PEs with” drop-down list, you can display PEs by Customer Name, by Site, or by Device Name.
- b. You can use the **Find** button to either search for a specific PE, or to refresh the display.
- c. You can set the “Rows per page” to **5, 10, 20, 30, 40**, or **All**.
- d. 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.

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, as shown in [Figure 6-6](#).

Figure 6-6 Specifying the MPLS Link Interface Attributes

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	pe1
Interface Name:	Ethernet4/0. (1-4294967295)
Interface Description:	
Shutdown Interface:	☐
Encapsulation:	DOT1Q v
VLAN ID [*] :	(1-4094)
Auto-Pick VLAN ID:	☐
Second VLAN ID: [?]	(1-4094)
Use SVI:	☐
CE Information	
CE	ce3
Interface Name:	Ethernet0/0. (1-4294967295)
Interface Description:	
Encapsulation:	DOT1Q v

211705

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 5-4.

Notes on the VLAN ID and Second VLAN ID Attributes

The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both.

The Second VLAN ID is an optional attribute that provides a method to match the Q-in-Q second VLAN tag of incoming frames on the PE interface.

Usage notes:

- This attribute is not available for service requests based on MVRFC policies.
- This attribute does not exist at the policy level and must be set while creating the service request. There is no corresponding autopick option for the second VLAN ID, so a value must be supplied. It must be an integer from 1 to 4094.
- This attribute is only applicable for regular PE-CE links. It is supported both when the CE is present and when it is not present. It is supported for both managed and unmanaged CE devices.
- This attribute is only applicable when the encapsulation type for the PE interface is dot1q. For all other encapsulation types, this attribute does not appear in GUI.
- The attribute does not appear in the GUI if the PE device is an IOS XR device.
- This feature is available for limited platforms (only those that support Q-in-Q matching). If service requests with second VLAN ID are deployed on unsupported platforms it results in a deployment failure. In such cases, the operator can remove the second VLAN ID and redeploy the service. This would be a service-affecting operation, since the IP address is also removed and redeployed during the change.
- A service request created with a second VLAN ID results in the following command on the device:
encapsulation dot1q VLAN_ID second-dot1q SECOND_VLAN_ID

- ISC does not apply the second VLAN. It only supports the second VLAN matching on the PE interface.
- The second VLAN ID attribute is available for use as a template variable.



Note For additional information on second VLAN ID and Q-in-Q support, see [Appendix A, “Sample Configlets” \(CE-PE L3 MPLS VPN \(Q-in-Q/Second VLAN ID\), page A-16\)](#) and [Frequently Asked Questions, page C-2](#).

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. 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 the IP Address Scheme, page 5-8](#).

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, as shown in [Figure 6-7](#).

Figure 6-7 Specifying the MPLS Link Routing Protocol Attributes

Attribute	Value
PE-CE Ipv4 Routing Information	
Routing Protocol	RIP
CsC Support:	☒
Give Only Default Routes to CE:	☒
Redistribute Static (BGP only):	☒
Redistribute Connected (BGP only):	☒
Redistributed Protocols on PE:	Edit
Redistributed Protocols on CE:	Edit

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 and CE, see [Specifying the Routing Protocol for a Service, page 5-11](#).

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 [Setting Static Routing Protocol Attributes \(for IPv4 and IPv6\), page 6-13](#).

Step 15 Edit any routing protocol values that must be modified for this particular link, then click **Next**.



Note If this interface is dual stacked (IPv4 and IPv6), you will be prompted to enter the routing information for both IPv4 and IPv6 independently.

The MPLS Link Attribute Editor for the VRF and VPN attributes appears. 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 VRF and VPN Information, page 5-29](#).

**Note**

If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Step 16 If multicast is enabled, choose the PIM (Protocol Independent Multicast) Mode:

- SPARSE_MODE
- SPARCE_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.

Step 18 Click the **Next** button if you want to associate templates or data files to the service request.

The Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) When you have completed setting up templates and data files for the device(s), click **Finish** in the Template Association window to close it and return to the Service Request Editor window.

Step 19 If you did not add templates, click **Finish** in the MPLS Link Editor – VRF and VPN window.

You return to the MPLS Service Request Editor. You can define multiple links in this service request, following the steps outlined in previous steps.

Step 20 To save your work on this first link in the service request, click **Save**.

You return to the Service Requests window, where the information for the link you just defined is now displayed, as shown in [Figure 6-8](#).

Figure 6-8 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									
#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	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

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 6-25](#).

**Note**

By default, all service requests in the ISC system are shown in the Service Request window. You can filter the list of service requests to be displayed by choosing different selections from the **Show Services with**, **matching**, and **of type** drop-down lists and clicking the **Find** button.

**Note**

If you have only ACTIVATION, L3MPLSVPN, and VPN licenses installed for ISC, you cannot display all service requests based on the VPN used (by choosing **VPN Name** in the **Show Services with** drop-down list, where **Type** is **All**). The workaround for this is to display the service requests based the MPLS VPN type (by choosing **MPLS VPN** in the **of type** drop-down list). This problem does not occur if all ISC licenses are installed.

Viewing Configlets Generated by the MPLS VPN Service Request

To view configlets generated on the PE and CE device by the MPLS VPN service request, perform the following steps.

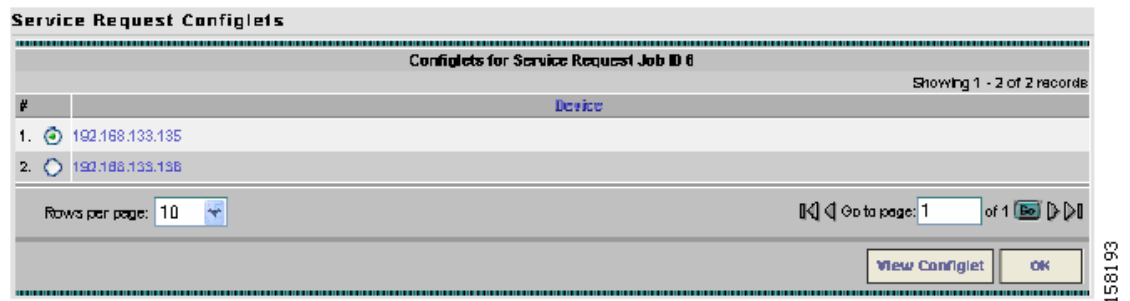
Step 1 To view the PE and CE configlets for a service request that has been successfully deployed, from the Service Request window, choose the service request you want to see, then click **Details**.

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, as shown in [Figure 6-9](#).

Figure 6-9 Service Request Configlets



Step 3 Choose the IP address for the desired configlet, then click **View Configlet**.

For additional information about viewing device configlets for a deployed service request, see [Viewing Configlets Generated by a Service Request, page 6-31](#). For sample configlets, see [Appendix A, “Sample Configlets.”](#)

Setting Static Routing Protocol Attributes (for IPv4 and IPv6)

For the static routing protocol, in addition to the attributes that you can specify in the service policy, there are 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 space 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 space throughout the VPN.

IPv4 Routing Information

For configuring IPv4 routing information, perform the following steps.

- 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 6-10](#)).

Figure 6-10 Static Routing Protocol (IPv4)

Attribute	Value
PE-CE IPv4 Routing Information	
Routing Protocol	STATIC
CsC Support:	☐
Give Only Default Routes to CE:	☐
Redistribute Connected (BGP only):	☐
Default Information Originate (BGP only):	☒
Advertised Routes for CE:	Edit
Routes To Reach Other Sites:	Edit
Next Hop Option:	USE_OUTGOING_INTF_NAME

Note: * - Required Field

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.
- Step 3** Click **Add** to add IP addresses.
The Advertised Routes window appears again.
- Step 4** Enter an IP address and a metric.
- Step 5** Click **Add** to add another IP address or click **OK**.
- Step 6** To edit **Routes to Reach Other Sites:**, click **Edit**.
The Routes to reach other sites window appears.
- Step 7** Click **Add** to add IP addresses.
The Routes to reach other sites window appears again.
- Step 8** Enter an IP address and a metric.
- Step 9** Click **Add** to add another IP address or click **OK**.
- Step 10** Choose a Next Hop Option:
- USE_OUT_GOING_INTF_NAME
 - USE_NEXT_HOP_IPADDR

IPv6 Routing Information

For configuring IPv6 routing information, perform the following steps.

- 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 6-11](#)).

Figure 6-11 Static Routing Protocol (IPv6)

Attribute	Value
PE-CE IPv6 Routing Information	
Routing Protocol	STATIC
Give Only Default Routes to CE:	☐
Redistribute Connected (BGP only):	☐
Default Information Originate (BGP only):	☐
Advertised Routes for CE:	Edit
Next Hop Option:	USE_NEXT_HOP_IPADDR
Next Hop IP Address *	(a:b:c:d:e:f:gh)

Note: * - Required Field

You can edit **Advertised Routes for CE:** for this service request.

- Step 2** To edit **Advertised Routes for CE:**, click **EDIT**.

The Advertised Routes window appears.

- Step 3** Click **Add** to add IP addresses.

The Advertised Routes window appears again.

- Step 4** Enter an IP address and a metric.

- Step 5** Click **Add** to add another IP address or click **OK**.

- Step 6** Click **Add** to add IP addresses.

- Step 7** Click **Add** to add another IP address or click **OK**.

- Step 8** Choose a Next Hop Option:

- USE_OUT_GOING_INTF_NAME
- USE_NEXT_HOP_IPADDR

- Step 9** Enter an IP address (in IPv6 format) in the **Next Hop IP Address:** field.

For information on formats supported formats for entering IPv6 addresses, see [MPLS VPN Service Policies, page 4-9](#).

Creating a Multi-VRF Service Request

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.

To create a Multi-VRFCE PE-CE service request, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears.

Step 2 From the **Create** drop-down list, choose **MPLS VPN**.

The Select MPLS Policy window appears.

Step 3 Choose the MPLS Policy. (**mvrfce pe-ce**)

Step 4 Click **OK**.

The MPLS Service Request Editor window appears.

Step 5 Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in [Figure 6-12](#).

Figure 6-12 MPLS Service Request Editor - Select CE

#	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	[dropdown]	[dropdown]	Select MVRFCE	[dropdown]	Select PE	[dropdown]	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 6 Click **Select CE**.

The Select CPE Device - CE window appears.

Step 7 Choose the **CPE Device** (mlce4) and then click **Select**.

The MPLS Service Request Editor window appears, as shown in [Figure 6-13](#).

Figure 6-13 MPLS Service Request Editor - CE Interface

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	mlce4	FastEthernet0/1		Select MVRFCE		Select PE		Add	N/A

Rows per page: 10

Go to page: 1 of 1 [Go](#)

[Add Link](#) [Delete Link](#) [Save](#) [Cancel](#)

116130

Step 8 Choose the **CE Interface** from the drop-down box.

Step 9 Click **Select MVRFCE**.

The Select CPE Device - MVRFCE window appears.

Step 10 Choose the **MVRFCE** and then click **Select**.

The MPLS Service Request Editor window appears, as shown in [Figure 6-14](#).

Figure 6-14 MPLS Service Request Editor - MVRFCE CE Facing Interface

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	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Select One	Select PE		Add	N/A

Rows per page: 10

Go to page: 1 of 1 [Go](#)

[Add Link](#) [Delete Link](#) [Save](#) [Cancel](#)

116132

Step 11 Choose the **MVRFCE CE Facing Interface** from the drop-down box.

The MPLS Service Request Editor window appears, as shown in [Figure 6-15](#).

Figure 6-15 MPLS Service Request Editor - Choose MVRFCE PE Facing Interface

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	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	Select PE		Add	N/A

Rows per page: 10

Go to page: 1 of 1 [Go](#)

[Add Link](#) [Delete Link](#) [Save](#) [Cancel](#)

116134

Step 12 Click **Select PE**.

The Select PE Device window appears.

Step 13 Choose the **PE** and then click **Select**.

The MPLS Link Attribute Editor window appears, as shown in Figure 6-16.

Figure 6-16 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

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

Add Link Delete Link Save Cancel

Step 14 Choose the **PE Interface** from the drop-down box.

Step 15 Click **Add** in the **Link Attribute** cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 6-16.

Figure 6-17 MPLS Link Attribute Editor - Interface

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	mlpe2
Interface Name:	FastEthernet0/0
Interface Description:	
Shutdown Interface:	☐
Encapsulation:	DOT1Q
VLAN ID *	510 (1-4095)
MVRFCE PE Facing Information	
MVRFCE	mlce3
Interface Name:	Ethernet0/1
Interface Description:	
Encapsulation:	DOT1Q

Note: * - Required Field

- Step 1 of 7 -

< Back Next > Finish Cancel

Step 16 Enter the VLAN ID for the PE. (**510**)

Step 17 Click **Next**.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 6-18.

Figure 6-18 MPLS Link Attribute Editor - Interface

MPLS Link Attribute Editor - Interface

Attribute	Value
MVRFCE CE Facing Information	
MVRFCE	mlce3
Interface Name:	Ethernet0/2.
Interface Description:	
Encapsulation:	DOT1Q v
VLAN ID *:	530 (1-4095)
CE Information	
CE	mlce4
Interface Name:	FastEthernet0/1.
Interface Description:	
Encapsulation:	DOT1Q v

Note: * - Required Field

- Step 2 of 7 -

116138

Step 18 Enter the VLAN ID for the MVRFCE (530).

Step 19 Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears.

Step 20 Keep the defaults, and click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears.

Step 21 Keep the defaults, and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears.

Step 22 Keep the defaults and click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears.

Step 23 Click **Add** to choose a VPN.

The Select VPN window appears.

Step 24 Choose a **VPN**.

Step 25 Click **Join as Hub** or **Join as Spoke** to join the CERC.

Step 26 Click **Done**.

The MPLS Link Attribute Editor - VRF and VPN window reappears.

Step 27 Click the **Next** button if you want to associate templates or data files to the service request.

The Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) When you have completed setting up templates and data files for the device(s), click **Finish** in the Template Association window to close it.

The Service Request Editor window appears.

- Step 28** If you did not add templates, click **Finish** in the MPLS Link Editor – VRF and VPN window.
The MPLS Service Request Editor window appears, as shown in [Figure 6-19](#).

Figure 6-19 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 Facing Interface	MVRFCFCE	MVRFCFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	6	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Edited	Details...

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

Add Link Delete Link Save Cancel

- Step 29** Enter the service request description and then click **Save**.

The MPLS Service Requests window appears showing that the service request is in the Requested state and ready to deploy.

Creating a PE-Only Service Request

To create a PE-only service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.
The Service Requests window appears.
- Step 2** To start the process to create a new service, click **Create**.
A drop-down list appears, showing the types of service requests you can create.
- Step 3** Choose **MPLS VPN**.
The Select MPLS Policy dialog box appears. This dialog box displays the list of all the MPLS service policies that have been defined in ISC.
- Step 4** Choose the policy that has CE *not* present, then click **OK**.
The MPLS Service Request Editor appears.
- Step 5** Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields, as shown in [Figure 6-20](#). 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 to a Service Request”](#) section on page 6-25.

Figure 6-20 Initial Fields Displayed to Define PE-Only Link

The screenshot shows the 'MPLS Service Request Editor' window. At the top, it says 'Showing 1-1 of 1 records'. Below this is a table with the following columns: #, Link ID, CLE, CLE Interface, PE, PE Interface, Link Attribute, and Logical Link. The first row shows: 1., 0, Select CLE, a dropdown arrow, Select PE, a dropdown arrow, Add, and N/A. Below the table is a 'Rows per page:' dropdown set to 10. At the bottom right are buttons: Add Link, Delete Link, Save, and Cancel.

Step 6 PE: Click **Select PE**.

The Select PE Device dialog box appears.

- 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.

Step 8 PE Interface: Choose the PE interface from the drop-down list, as shown in [Figure 6-21](#).

Figure 6-21 PE and PE Interface Fields Defined

The screenshot shows the 'MPLS Service Request Editor' window. At the top, it says 'Showing 1-1 of 1 records'. Below this is a table with the following columns: #, Link ID, CLE, CLE Interface, PE, PE Interface, Link Attribute, and Logical Link. The first row shows: 1., 0, Select CLE, a dropdown arrow, mlpe2, Serial3/1, Add, and N/A. Below the table is a 'Rows per page:' dropdown set to 10. At the bottom right are buttons: Add Link, Delete Link, Save, and Cancel.

Note that the Link Attribute **Add** option is now enabled.

Step 9 In the Link Attribute column, click **Add**.

The MPLS Link Attribute Editor appears, showing the fields for the interface parameters, as shown in Figure 6-22.

Figure 6-22 Specifying the PE-Only Link Interface Attributes

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	pe1
Interface Name:	Ethernet4/0. (1-4294967295)
Interface Description:	
Shutdown Interface:	☒
PE Encapsulation:	DOT1Q
Auto-Pick VLAN ID:	☒
Second VLAN ID:	(1-4094)
Use SVI:	☐
Standard UNI Port:	☒
UNI Security Information	
Disable CDP:	☐
Filter BPDUs:	☐
Use Existing ACL Name:	☐
UNI MAC Addresses:	Edit
UNI Port Security:	☒
Maximum MAC Address:	(1 - 5120)
Aging (in minutes):	(0 - 1440)
Violation Action:	PROTECT
Secure MAC Addresses:	Edit

211706

The field values displayed in this window 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 5-4](#).



Note For information on setting the VLAN ID and Second VLAN ID attributes, see [Notes on the VLAN ID and Second VLAN ID Attributes, page 6-10](#).

Step 10 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. 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 the IP Address Scheme, page 5-8](#).

Step 11 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, as shown in [Figure 6-23](#).

Figure 6-23 Specifying the PE-Only Routing Protocol Attributes (IPv4)

MPLS Link Attribute Editor - Ipv4 Routing Information

Attribute	Value
PE-CE Ipv4 Routing Information	
Routing Protocol	BGP
CsC Support:	☐
Redistribute Static (BGP only):	☐
Redistribute Connected (BGP only):	☐
Site of Origin:	☒
Value :	Select
Neighbor IP Address :	(a.b.c.d)
CE BGP AS ID :	(1-65535)
Neighbor Allow-AS In:	(1-10)
Neighbor AS Override:	☐
Advertise Interval:	(1-600 Seconds)
Max Prefix Number:	(1-2147483647)
Max Prefix Threshold:	(1-100 %)
Max Prefix Warning Only:	☐
Max Prefix Restart:	(1-65535 Minutes)

Note: * - Required Field

211618

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 the Routing Protocol for a Service, page 5-11](#).

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 12 If you check **Site of Origin**, the screen updates to include the required step of selecting a value:

a. Click **Select**.

The Site for SOO Value window appears.

b. From the available list shown, check the check box associated with a site and its SOO value, then click **Select**.

Step 13 Edit any routing protocol values that must be modified for this particular link.



Note If this interface is dual stacked (IPv4 and IPv6), you will be prompted to enter the routing information for both IPv4 and IPv6 independently.

When specifying IPv6 routing protocol information, the MPLS Link Attribute Editor for Routing Information shows only a subset of options, as shown in [Figure 6-24](#). For information on formats supported for entering IPv6 addresses, see [MPLS VPN Service Policies, page 4-9](#).

Figure 6-24 Specifying the PE-Only Routing Protocol Attributes (IPv6)

Attribute	Value
PE-CE IPv6 Routing Information	
Routing Protocol	BGP
Redistribute Static (BGP only):	☐
Redistribute Connected (BGP only):	☐
Neighbor IPv6 Address/Mask *	(a:b:c:d:e:f:g:h)
CE BGP AS ID *	(1-65535)
Neighbor Allow-AS In:	(1-10)
Neighbor AS Override:	☐

Note: * - Required Field

Step 14 Click **Next**.

The MPLS Link Attribute Editor for the VRF and VPN attributes appears. 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 VRF and VPN Information](#), page 5-29.

**Note**

If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Step 15 Edit any VRF and VPN values that must be modified for this particular link.

Step 16 Click the **Next** button, if you want to associate templates or data files to the service request.

The Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) When you have completed setting up templates and data files for the device(s), click **Finish** in the Template Association window.

The Service Request Editor window appears. You can define multiple links in this service request by following the steps outlined in the previous steps.

Step 17 If you did not add templates, click **Finish** in the MPLS Link Editor – VRF and VPN window.

The Service Request Editor window appears.

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.

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 6-25.

Adding a CLE to a Service Request

To add a CLE device to the service request described in [Creating a PE-Only Service Request, page 6-20](#), perform the following steps.

-
- Step 1** Follow [Step 1](#) through Step 5 of [Creating a PE-Only Service Request, page 6-20](#).
- Step 2** Click **Select CLE**. The Select PE Device dialog box appears.
- 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 6](#) through [Step 18](#) of “[Creating a PE-Only Service Request](#)” section on [page 6-20](#).
-

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.

To deploy the service requests immediately or schedule their deployment, perform the following 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.
- 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
- 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.

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, as shown in [Figure 6-25](#).

Figure 6-25 *Scheduling a Service Request for Deployment*

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 6-26](#).

Figure 6-26 *Status for Successful Deployment*

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, see the [Cisco IP Solution Center Infrastructure Reference, 5.1.](#))

Monitoring Service Requests

After you have created and deployed a service request, to monitor its status, perform the following steps.

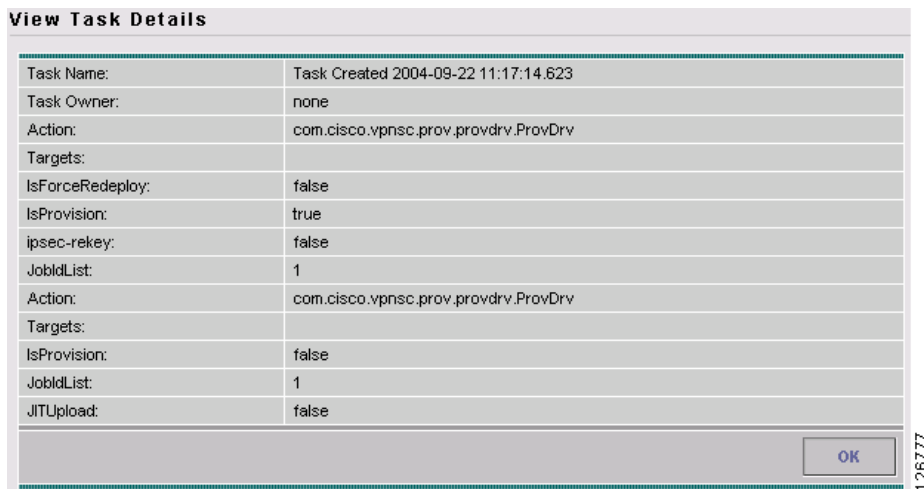
- Step 1** Click the **Monitoring** tab.
- Step 2** From the Monitoring window, choose **Task Manager**.
- The Task Manager dialog box appears, as shown in [Figure 6-27](#).

Figure 6-27 Viewing Information on Running Tasks

Tasks					
Show Tasks with Task Name matching of Type Find					
Showing 1 - 10 of 11 records					
#	☐	Task Name	Type	Schedule	Creator
1.	☐	Task Created 2004-09-28 10:07:55.103	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD
2.	☐	Task Created 2004-09-28 10:03:09.686	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD
3.	☐	Task Created 2004-09-28 09:58:02.981	Service Deployment	Single run at 2004-09-28 09:58:00.0	SD
4.	☐	Task Created 2004-09-28 09:51:34.271	Service Deployment	Single run at 2004-09-28 09:51:00.0	SD
5.	☐	Collect Config 2004-09-27 17:05:47.503	Collect Config	Single run at 2004-09-27 17:06:00.0	ENG
6.	☐	Task Created 2004-09-22 11:37:56.332	Service Deployment	Single run at 2004-09-22 11:37:00.0	SD
7.	☐	Task Created 2004-09-22 11:35:10.21	Service Deployment	Single run at 2004-09-22 11:35:00.0	SD
8.	☐	Task Created 2004-09-22 11:29:16.333	Service Deployment	Single run at 2004-09-22 11:29:00.0	SD
9.	☐	Task Created 2004-09-22 11:24:33.102	Service Deployment	Single run at 2004-09-22 11:24:00.0	SD
10.	☐	Task Created 2004-09-22 11:17:14.623	Service Deployment	Single run at 2004-09-22 11:17:00.0	SD
Rows per page: 10 Go to page: 1 of 2 Go					
Auto Refresh: ☒ Create Audit Details Schedules Delete					

126725

- Step 3** Check the check box for the service request in which you are interested.
- Step 4** To see details about the service request deployment, click **Details**.
- The Service Request Details window appears, as shown in [Figure 6-28](#).

Figure 6-28 Service Request Details Displayed

The screenshot shows a 'View Task Details' dialog box with a table of task information. The table has two columns: 'Task Name:' and 'Task Created 2004-09-22 11:17:14.623'. The rows contain the following data:

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

At the bottom right of the dialog box is an 'OK' button. The number '126777' is visible on the right side of the dialog box.

Auditing Service Requests

This section describes auditing in MPLS VPN. It contains the following sections:

- [Functional Audit, page 6-28](#)
- [Configuration Audit, page 6-29](#)

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.

To create a task to do a functional audit for one or more service requests, perform the following steps.

- Step 1** Choose **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 uncheck 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 Functional Audit

To display the Functional audit report, perform the following 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 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 configuration audit whenever a service request is deployed or force-redeployed. To create a task to do a configuration audit for one or more service requests, perform the following steps.

Step 1 Choose **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 Configuration Audit

To display the Configuration audit report, perform the following steps.

Step 1 Choose a service request, and click **Details**.

On the Service Request Details page, the Audit button has two choices:

- Config
- Functional

Step 2 Click **Config** to display the Configuration audit report.

Why 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.

Another reason a configuration audit can fail is if ISC does not recognize commands in the configuration file. The default behavior in ISC is to skip unrecognized commands in the configuration file during the configuration audit. Such unrecognized commands might have been present in an existing configuration or manually inserted in the configuration file. If an unrecognized command is at the start of a block of commands, ISC will skip the initial command and continue to parse the subcommands in the block. This might lead ISC to assume there is an error in the logic flow within the configuration file and cause the audit to fail.

Viewing Configlets Generated by a Service Request

To view configlets that have been generated by a service request for a device, perform the following steps.

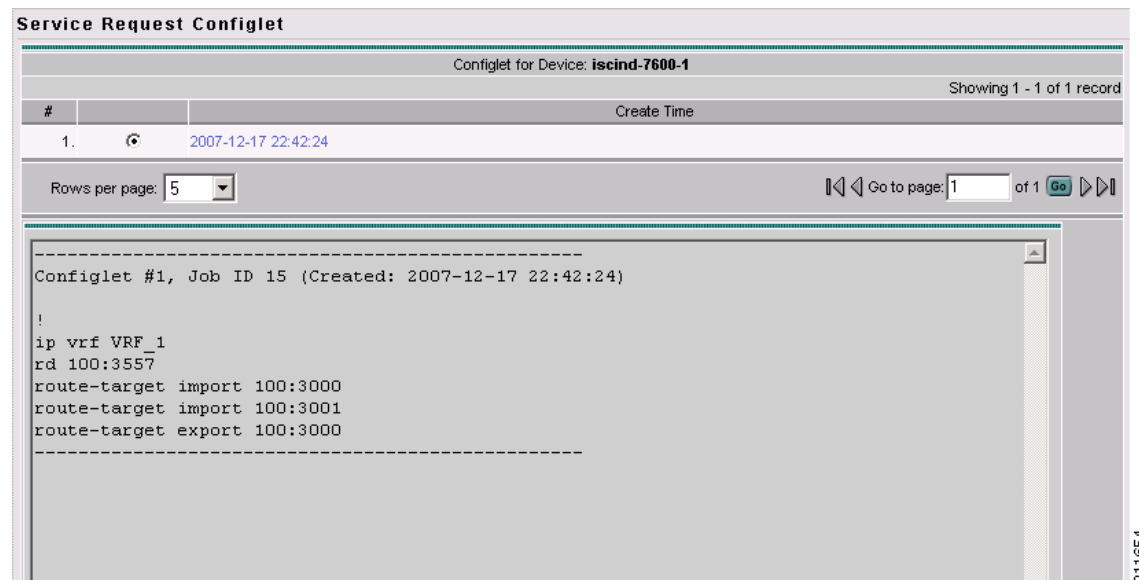


Note

For IOS devices, the configlets will appear as CLI commands. For IOS XR devices, the configlets can be viewed in XML or CLI format. For information about viewing configlets for IOS XR devices, see [Viewing Configlets on IOS XR Devices, page 6-32](#).

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to view the available service requests.
- Step 2** Check the appropriate check box to select the service request for which you want to view the associated configlets.
- Step 3** Click the **Details** button.
The Service Request Details window appears.
- Step 4** Click the **Configlets** button.
The Service Request Configlets window appears. This window displays a list of devices for which configlets have been generated.
- Step 5** To view configlets that were generated for a device, select a device and click the **View Configlet** button.
The Service Request Configlet window updates showing the configlet, as shown in [Figure 6-29](#). By default, the latest generated configlet is displayed.

Figure 6-29 Service Request Configlet Window



- Step 6** If applicable, you can display configlets for a device based on the time of creation. Choose the desired time of creation in the Create Time list to display a specific configlet based on the time the configlet was generated for the service request.

Step 7 Click **OK** when you are finished viewing the configlet.

Viewing Configlets on IOS XR Devices

By default, service requests for IOS XR devices log the configuration sent to the device in XML format. Therefore, when configlets are viewed for IOS XR devices, they are displayed in raw XML format. ISC also allows the configlet to be viewed in CLI format. This feature is enabled by setting the DCPL property **DCS/getCommitCLIConfigAfterDownload** to true (which is the default setting).

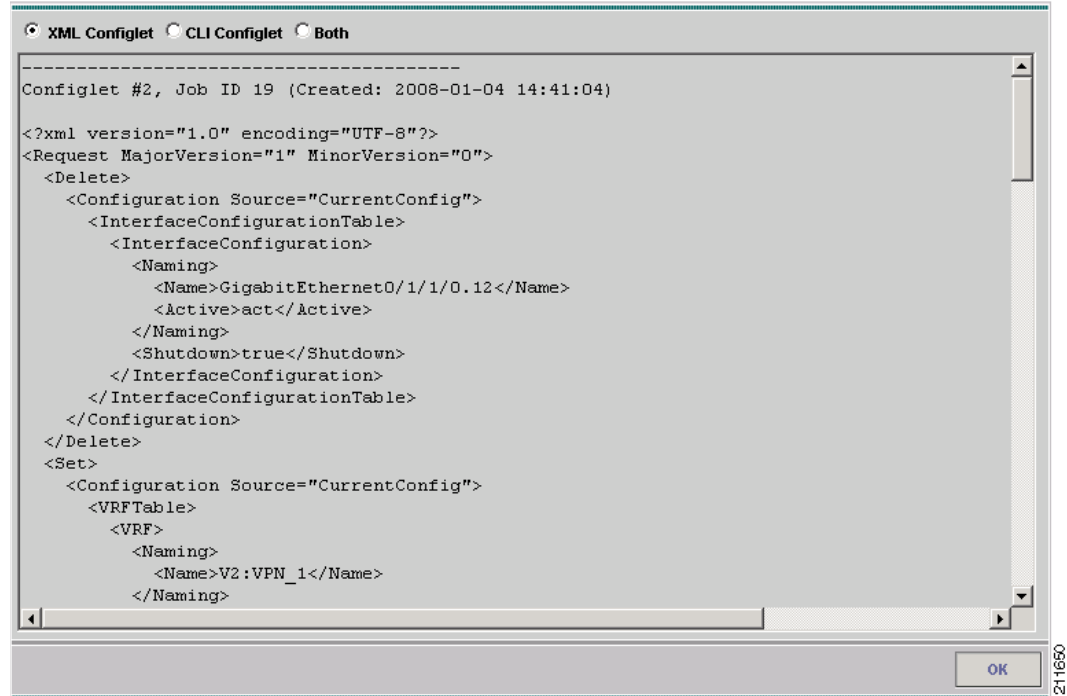


Note

The DCPL property **DCS/getCommitCLIConfigAfterDownload** must be set to true to display the configlet(s) in CLI format. On setting the DCPL property to true, CLI configlets will only be available for subsequent service request deployments. They will not be available for configlets that were deployed before the DCPL property was set to true.

To view the configlets for IOS XR devices in XML or CLI formats, or both, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to view the available service requests.
 - Step 2** Check the appropriate check box to select the service request for which you want to view the associated configlets.
 - Step 3** Click the **Details** button.
The Service Request Details window appears.
 - Step 4** Click the **Configlets** button.
The Service Request Configlets window appears. This window displays a list of devices for which configlets have been generated.
 - Step 5** To view configlets that were generated for an IOS XR device, select an IOS XR device and click the **View Configlet** button.
The Service Request Configlet window appears showing the configlet in CLI format. By default, the latest generated configlet is displayed.
 - Step 6** If applicable, you can display configlets for a device based on the time of creation. Choose the desired time of creation in the Create Time list to display a specific configlet based on the time the configlet was generated for the service request.
 - Step 7** To view the configlet in XML format, click the **XML Configlet** radio button.
The window refreshes and displays the configlet in XML format, as shown in [Figure 6-30](#).

Figure 6-30 Service Request Configlet Window (with Configlet in XML Format)

- Step 8** To toggle among different formats, use the following radio buttons:
- **XML Configlet**—Displays the configlet in XML format.
 - **CLI Configlet**—Displays the configlet in CLI format. This the default selection.
 - **Both**—Displays the configlet side by side in both XML and CLI formats.
- Step 9** Click **OK** when you are finished viewing the configlet.

Editing Configuration Files

To view or edit an existing router configuration file, perform the following steps.



Note

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.
- Step 2** Choose **Inventory and Connection Manager**.
- The Inventory and Connection Manager window appears.
- Step 3** Click **Devices**.
- The Devices dialog box appears as shown in [Figure 6-31](#).

Figure 6-31 List of Devices Recognized by ISC

You Are Here: [Service Inventory](#) > [Inventory and Connection Manager](#) > [Devices](#) Customer: None

Devices

Show Devices with Matching

Showing 1 - 10 of 27 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	mlce3	172.29.146.26	Cisco IOS Device	
2.	☐	mlpe1		Cisco IOS Device	
3.	☐	mlpe2		Cisco IOS Device	
4.	☒	mlpe3	172.29.146.23	Cisco IOS Device	
5.	☐	mlpe4	172.29.146.41	Cisco IOS Device	
6.	☐	mlce4		Cisco IOS Device	
7.	☐	mlsw2	172.29.146.38	Cisco IOS Device	
8.	☐	mlsw1	172.29.146.37	Cisco IOS Device	
9.	☐	mlsw3	172.29.146.39	Cisco IOS Device	
10.	☐	mlsw4	172.29.146.40	Cisco IOS Device	

Rows per page:

Step 4 Check the check box next to the device name to choose the configuration file versions you want to view.

Step 5 Click **Config**.

The Device Configurations dialog box appears, as shown in [Figure 6-32](#).

Figure 6-32 List of Configurations for the Selected Device

Device Configurations

Device: mlpe3 Allowed Configs: unlimited

Showing 1 - 2 of 2 records

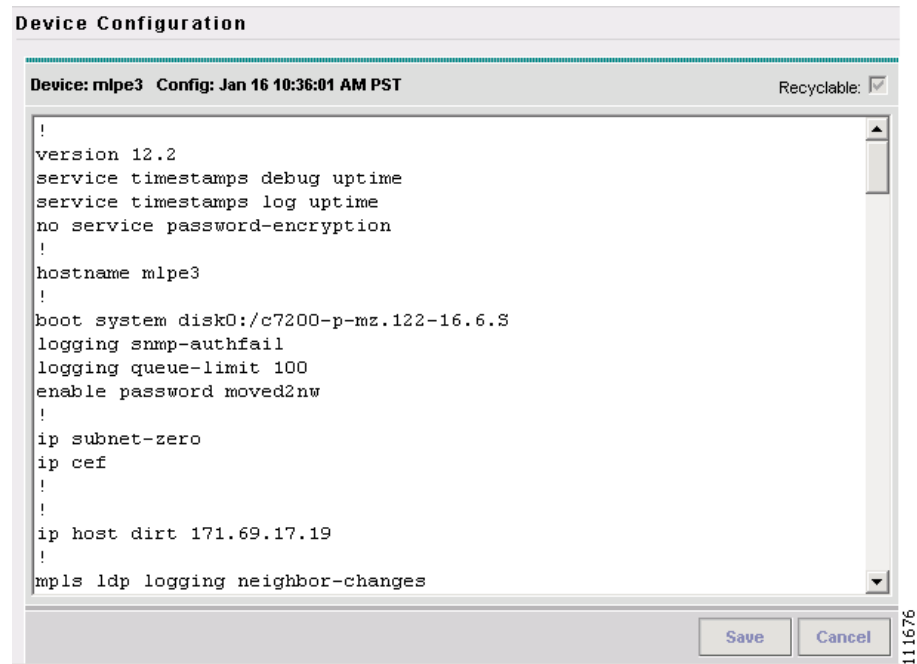
#	☐	Date	Recyclable
1.	☐	Jan 20 02:10:54 PM PST	Yes
2.	☐	Jan 16 10:36:01 AM PST	Yes

Rows per page:

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 6 Choose the version of the configuration file you want to view, then click **Edit**.

The contents of the selected configuration file are displayed, as shown in [Figure 6-33](#).

Figure 6-33 *Selected Configuration Displayed*

You can view or edit the displayed device configuration file.

- Step 7** If necessary, edit the configuration file.
- Step 8** When finished editing the file, click **Save**.



CHAPTER 7

Provisioning Regular PE-CE Links

This chapter describes how to configure MPLS VPN PE-CE links in the IP Solution Center (ISC) provisioning process. It contains the following major sections:

- [MPLS VPN PE-CE Link Overview, page 7-1](#)
- [Creating MPLS VPN PE-CE Service Policies, page 7-3](#)
- [Creating MPLS VPN PE-CE Service Requests, page 7-8](#)

MPLS VPN PE-CE Link Overview

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.

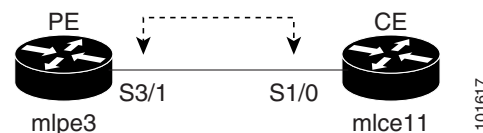
ISC supports two MPLS VPN Service Policy Types: Regular PE-CE and MVRFCE PE-CE. The following scenarios focus on the Regular PE-CE Policy Type.

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)

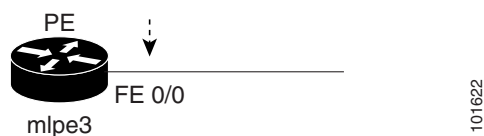
[Figure 7-1](#) shows an example of a normal PE to CE link between two devices.

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.

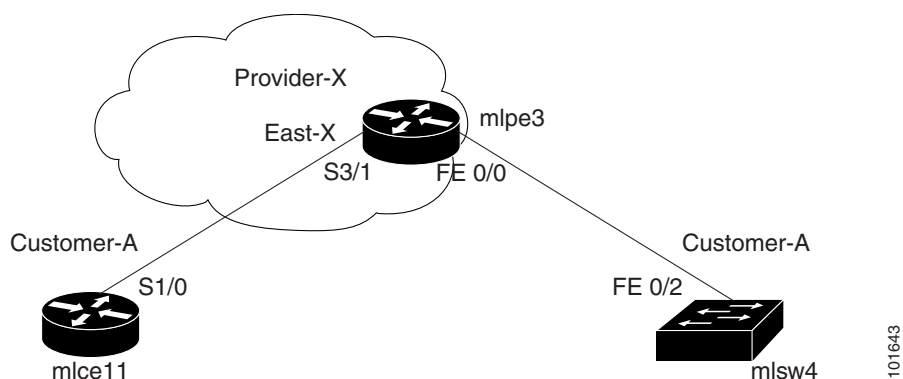
[Figure 7-2](#) shows an example of a PE Only link with no CE.

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 Service Inventory tasks:

-
- Step 1** Set up a Customer with a Site (see [Creating Customers, Sites, and CPEs](#), page 2-7).
 - Step 2** Setup a Provider with a Region (see [Creating Providers, Regions, and PEs](#), page 2-9).
 - Step 3** Import, create, or discover Devices (see [Creating Devices](#), page 2-2).
 - Step 4** Create CPE and PE (see [Creating CPEs](#), page 2-8).
 - Step 5** Collect Configurations (see [Collecting Configurations](#), page 2-4).
 - Step 6** Create Resource Pools (see [Creating Resource Pools](#), page 2-15).
 - Step 7** Create CE routing communities (CERC) (see [Creating CE Routing Communities](#), page 2-32).
 - Step 8** Define a MPLS VPN (see [Creating an MPLS VPN](#), page 2-22).
-

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.

To define a VPN, perform the following steps.

-
Step 1	Choose Service Inventory > Inventory and Connection Manager > VPNs . The VPN window appears.
Step 2	Click Create to create a VPN. The Create VPN window appears.
Step 3	In the Name field, enter the VPN name. It is recommended not to use special characters (' ` " < > () [] { } / \ & ^ ! ? ~ * % = , . +) in the VPN name, as this may cause misconfiguration of the VRF name for certain devices, if the VPN name is used to autogenerate a VRF name.
Step 4	In the Customer field, click Select . The Select Customer window appears.
Step 5	Check to choose a Customer and click Select . The VPNs window reappears where the new VPN Name is associated with a Customer in this new VPN definition.
Step 6	Click Save .
-

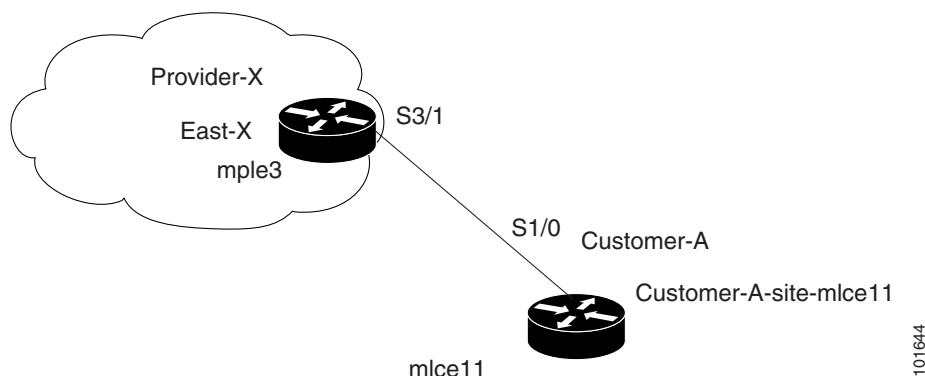
Creating MPLS VPN PE-CE Service Policies

This section contains the following sections:

- [PE-CE Service Policy Overview, page 7-3](#)
- [Creating a PE-CE Service Policy, page 7-4](#)
- [Creating a PE-NoCE Service Policy, page 7-6](#)

PE-CE Service Policy Overview

[Figure 7-4](#) shows an example of the PE-CE link that is defined in the PE-CE Service Policy scenario.

Figure 7-4 PE-CE Topology

Creating a PE-CE Service Policy

To create a PE-CE service policy, perform the following steps.

- Step 1** Choose **Service Design > Policies**.
The Policies window appears.
- Step 2** From the **Create** drop-down list, choose **MPLS Policy**.
The MPLS Policy Editor - Policy Type window appears, as shown in [Figure 7-5](#).

Figure 7-5 MPLS Policy Editor - Policy Type

Attribute	Value
Policy Name *	mpls-pe-ce
Policy Owner:	☒ Customer ☐ Provider ☐ Global Policy
Customer *	Select
Policy Type:	☒ Regular: PE-CE ☐ MVRFCPE: PE-CE
CE Present:	☒

Note: * - Required Field

- Step 3** Edit the following attributes:
- **Policy Name:** Enter the policy name.
 - **Policy Owner:** Choose the Policy Owner.
 - **Customer:**
 - Click **Select** to specify a Customer.

The Customer for MPLS Policy window appears.

- Check to choose a Customer and click **Select**.

- **Policy Type:** Choose the Policy Type. (**Regular PE-CE**)

Step 4 **CE Present:** Check to set CE as present.

Step 5 Click **Next**.

The MPLS Policy Editor - Interface window appears, as shown in [Figure 7-6](#).

Figure 7-6 *The MPLS Policy Editor - Interface*

MPLS Policy Editor - Interface

Attribute	Value	Editable
Reset All Attribute Editable Flags:		☒
PE Information		
Interface Type:	ANY	
Interface Format:		
Interface Description:		☒
Shutdown Interface:	☐	☒
Auto-Pick VLAN ID:	☐	☒
Use SVI:	☐	☒
Link Speed:	None	☒
Link Duplex:	None	☒
ETTH Support:	☐	☒
Standard UNI Port:	☒	☒
UNI Security Information		
Disable CDP:	☐	☒
Filter BPDU:	☐	☒
Use Existing ACL Name:	☐	
UNI MAC Addresses:	Edit	☒
UNI Port Security:	☒	☒
Maximum MAC Address:	(1 - 5120)	☒
Aging (in minutes):	(0 - 1440)	☒
Violation Action:	PROTECT	☒
Secure MAC Addresses:	Edit	☒
CE Information		
Interface Type:	ANY	
Interface Format:		
Interface Description:		☒

138950

Step 6 Click **Next** to accept the defaults.

The MPLS Policy Editor - IP Address Scheme window appears.



Note Make sure the Editable check boxes are checked, so you can edit these attributes in the service request process.

Step 7 Edit all applicable attributes.



Note If you check **Automatically Assign IP Address**, the screen refreshes and adds a forth attribute: **IP Address Pool**.

Step 8 Click **Next**.

The MPLS Policy Editor - Routing Information window appears.

Step 9 Click **Next** to accept the defaults.

The MPLS Policy Editor - VRF and VPN Membership window appears.



Note For information about protocol types, see [Specifying the Routing Protocol for a Service](#), page 5-11.



Note If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Step 10 To enable template association for the policy, click the **Next** button in MPLS Policy Editor - VRF and VPN Membership window.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) For additional information about using templates in ISC, also see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). When you have completed setting up templates and data files for the policy per the instructions in the appendix, click **Finish** in the Template Association window to close it.

The Policies window appears.

Step 11 If you did not enable templates, click **Finish** in the MPLS Policy Editor – VRF and VPN window.

The Policies window reappears.

The MPLS VPN PE-CE Service Policy is complete.

Creating a PE-NoCE Service Policy

To create a PE-NoCE service policy, perform the following steps.

Step 1 Choose **Service Design > Policies**.

The Policies window appears.

Step 2 From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in [Figure 7-7](#).

Figure 7-7 MPLS Policy Editor - Policy Type

MPLS Policy Editor - Policy Type

Attribute	Value
Policy Name *	mpls-pe-noce
Policy Owner:	☒ Customer ☐ Provider ☐ Global Policy
Customer *	CUST-A Select
Policy Type:	☒ Regular: PE-CE ☐ MVRFC: PE-CE
CE Present:	☐

Note: * - Required Field

101626

Step 3 Edit the following attributes:

- **Policy Name:** Enter the policy name.
- **Policy Owner:** Choose the Policy Owner.
- **Customer:**
 - Click **Select** to specify a Customer.
 - The Customer for MPLS Policy window appears.
 - Choose a Customer and click **Select**.
- **Policy Type:** Choose the Policy Type. (**Regular PE-CE**)
- **CE Present:** Do *not* check to set CE as **not** present (**NoCE**).

Step 4 Click **Next**.

The MPLS Policy Editor - Interface window appears.

Step 5 Click **Next** to accept the defaults.

The MPLS Policy Editor - IP Address Scheme window appears.



Note Make sure the Editable check boxes are checked, so you can edit these attributes in the service request process.

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 the IP Address Scheme, page 5-8](#).

Step 6 Edit all applicable attributes.



Note If you check **Automatically Assign IP Address**, the screen refreshes and adds a forth attribute: **IP Address Pool**.

Step 7 Click **Next**.

The MPLS Policy Editor - Routing Information window appears.

Step 8 Click **Next** to accept the defaults.

The MPLS Policy Editor - VRF and VPN Membership window appears.



Note For information about protocol types, see [Specifying the Routing Protocol for a Service, page 5-11](#).



Note If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Step 9 To enable template association for the policy, click the **Next** button in MPLS Policy Editor - VRF and VPN Membership window.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) For additional information about using templates in ISC, also see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). When you have completed setting up templates and data files for the policy per the instructions in the appendix, click **Finish** in the Template Association window to close it.

The Policies window appears.

Step 10 If you did not enable templates, click **Finish** in the MPLS Policy Editor – VRF and VPN window.

The Policies window reappears.

The MPLS VPN PE-NoCE Service Policy is complete.

Creating MPLS VPN PE-CE Service Requests

This section contains the following sections:

- [Creating PE-CE Service Requests, page 7-8](#)
- [Creating PE-NoCE Service Requests, page 7-12](#)

Creating PE-CE Service Requests

To create a PE-CE service request, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears.

Step 2 From the **Create** drop-down list, choose **MPLS VPN**.

The Select MPLS Policy window appears.

Step 3 Choose an MPLS PE-CE type policy.

Step 4 Click **OK**.

The MPLS Service Request Editor window appears.

Step 5 Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in [Figure 7-8](#).

Figure 7-8 MPLS Service Request Editor - Select CE

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: MPLSPolicy_PECE

Customer: Customer1

Description :

Showing 0 of 0 records

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
Showing 0 of 0 records							

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

[Add Link](#) [Delete Link](#) [Save](#) [Cancel](#)

Step 6 Click **Select CE**.

The CPE for MPLS VPN Link window appears.

Step 7 Choose a CPE device and click **Select**.

The MPLS Service Request Editor window appears.

Step 8 Choose a CE Interface from the drop-down list.

The MPLS Service Request Editor window appears.

Step 9 Click **Select PE**.

The PE for MPLS VPN Link window appears.

Step 10 Choose a PE device and click **Select**.

The MPLS Service Request Editor window appears.

Step 11 Choose a PE Interface from the drop-down list.

The MPLS Service Request Editor window appears.

Step 12 Click **Select PE**.

The PE for MPLS VPN Link window reappears.

Step 13 In the Link Attribute cell, click **Add**.

The MPLS Link Attribute Editor - Interface window appears, as shown in [Figure 7-9](#).

211708

Figure 7-9 MPLS Link Attribute Editor - Interface

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	pe1
Interface Name:	Ethernet4/0. (1-4294967295)
Interface Description:	
Shutdown Interface:	☒
Encapsulation:	DOT1Q v
VLAN ID *	(1-4094)
Auto-Pick VLAN ID:	☐
Second VLAN ID: ⓘ	(1-4094)
Use SVI:	☐
CE Information	
CE	ce3
Interface Name:	Ethernet0/0. (1-4294967295)
Interface Description:	
Encapsulation:	DOT1Q v

211707

PE Information

- Step 14 Interface Name:** Enter a value to identify the interface.
- Step 15 Interface Description:** Optionally, you can enter a description of the PE interface.
- Step 16 Shutdown Interface:** When you check this check box, the PE interface is configured in a shutdown state.
- Step 17 Encapsulation:** Choose the PE Encapsulation from the drop-down list.
- The selections available in the drop-down list are determined by the interface type.
- Step 18 VLAN ID:** Enter the VLAN ID. The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both.
- Step 19 Auto-Pick VLAN ID:** Check this check box if you would like ISC to autopick a VLAN ID from the VLAN pool.
- If this box is checked, the VLAN ID field is not visible in the GUI.
- Step 20 Second VLAN ID:** The Second VLAN ID is an optional attribute that provides a method to match the Q-in-Q second VLAN tag of incoming frames on the PE interface.
- For usage details about this attribute, see [Notes on the VLAN ID and Second VLAN ID Attributes, page 6-10](#).
- Step 21 Use SVI:** Check this box to have ISC terminate VRF on SVI.

CE Information

- Step 22 Interface Name:** Enter a value from to identify the interface.
- Step 23 Interface Description:** Optionally, you can enter a description of the PE interface.
- Step 24 Encapsulation:** Choose the CE Encapsulation from the drop-down list.
- The selections available in the drop-down list are determined by the interface type.
- Step 25** Click Next.

The MPLS Link Attribute Editor - IP Address Scheme window appears.

Step 26 Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window appears, as shown in [Figure 7-10](#).

Figure 7-10 MPLS Link Attribute Editor - Routing Information

MPLS Link Attribute Editor - Ipv4 Routing Information

Attribute	Value
PE-CE Ipv4 Routing Information	
Routing Protocol	STATIC ▾
CsC Support:	☒
Give Only Default Routes to CE:	☒
Redistribute Connected (BGP only):	☒
Default Information Originate (BGP only):	☐
Advertised Routes for CE:	Edit
Routes To Reach Other Sites:	Edit
Next Hop Option:	USE_OUTGOING_INTF_NAME ▾

Note: * - Required Field

Step 27 Choose a Next Hop Option:

- USE_OUT_GOING_INTF_NAME
- USE_NEXT_HOP_IPADDR



Note

If this interface is dual stacked (IPv4 and IPv6), you will be prompted to enter the routing information for both IPv4 and IPv6 independently. The fields in the IPv6 Routing Information window are slightly different from the IPv4 version. For information on setting up the routing information for IPv6, see [Setting Static Routing Protocol Attributes \(for IPv4 and IPv6\)](#), page 6-13.

Step 28 To continue, click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears.



Note

If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Step 29 Click **Add** to join a VPN.

The Select CERCs window appears.

Step 30 Choose a Customer from the drop-down list.

Step 31 Choose a VPN from the drop-down list.

Step 32 Check to choose a VPN from the list.

Step 33 Click **Join As Hub** or **Join As Spoke**.

Step 34 Click **Done**.

The MPLS Link Attribute Editor - VRF and VPN window reappears.

- Step 35** Click the **Next** button to associate templates or data files to the service request.



Note

This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 37, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#)

- Step 36** When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.

You can define multiple links in this service request, following the instructions outlined in previous steps.

- Step 37** To save your work, click **Save**.

The MPLS Service Requests window reappears showing that the MPLS VPN PE-CE service request is in the Requested state and ready to deploy.

Creating PE-NoCE Service Requests

To create a PE-NoCE service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears.

- Step 2** From the **Create** drop-down list, choose **MPLS VPN**.

The Select MPLS Policy window appears.

- Step 3** Choose an MPLS PE-NoCE type policy.

- Step 4** Click **OK**.

The MPLS Service Request Editor window appears.

- Step 5** Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in [Figure 7-11](#).

Figure 7-11 MPLS Service Request Editor - Select CE

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: MPLSPolicyNO_CE

Customer: Customer1

Description:

Showing 1 - 1 of 1 record

#	Link ID	UNI device	UNI Interface	PE	PE Interface	Link Attribute	Logical Link
1.	☐ 0	Select UNI Device	Select PE	Select PE		Add	N/A

Rows per page: 10

Go to page: 1 of 1

Step 6 Click **Select PE**.

The PE for MPLS VPN Link window appears.

Step 7 Choose a PE device and click **Select**.

The MPLS Service Request Editor window appears.

Step 8 Choose the PE Interface from the drop-down list.

The MPLS Service Request Editor window appears.

Step 9 In the Link Attribute cell, Click **Add**.

The MPLS Link Attribute Editor - Interface window appears, as shown in [Figure 7-12](#).

Figure 7-12 MPLS Link Attribute Editor - Interface

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	pe1
Interface Name:	Ethernet4/0. (1-4294967295)
Interface Description:	
Shutdown Interface:	☒
PE Encapsulation:	DOT1Q
VLAN ID *:	(1-4094)
Auto-Pick VLAN ID:	☐
Second VLAN ID:	(1-4094)
Use SVI:	☐
Standard UNI Port:	☐

Note: * - Required Field

Step 10 **Interface Name:** Enter a value to identify the interface.

Step 11 **Interface Description:** Optionally, you can enter a description of the PE interface.

Step 12 **Shutdown Interface:** When you check this check box, the PE interface is configured in a shutdown state.

Step 13 **PE Encapsulation:** Choose the PE Encapsulation from the drop-down list.

The selections available in the drop-down list are determined by the interface type. This field is needed for deciding PE/UNI encapsulation.

Step 14 VLAN ID: Enter the VLAN ID. The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both.

Step 15 Auto-Pick VLAN ID: Check this check box if you would like ISC to autopick a VLAN ID from the VLAN pool.

If this box is checked, the VLAN ID field is not visible in the GUI.

Step 16 Second VLAN ID: The Second VLAN ID is an optional attribute that provides a method to match the Q-in-Q second VLAN tag of incoming frames on the PE interface.

For usage details about this attribute, see [Notes on the VLAN ID and Second VLAN ID Attributes, page 6-10](#).

Step 17 Use SVI: Check this box to have ISC terminate VRF on SVI.

Step 18 Standard UNI Port: Check this box to access additional UNI security parameters.

Step 19 Choose the PE Encapsulation from the drop-down list.



Note This field is needed for deciding PE/UNI encapsulation.

Step 20 In the VLAN ID field, enter a valid value, or check **Auto-Pick VLAN ID**.

Step 21 Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears.

Step 22 Accept the defaults and click **Next**.



Note If this interface is dual stacked (IPv4 and IPv6), you will be prompted to enter the routing information for both IPv4 and IPv6 independently.

The MPLS Link Attribute Editor - Routing Information window appears. In the Hop Option field, you have the following options:

- For a point-to-point interface you have two options:
 - USE_OUT_GOING_INTF_NAME
 - USE_NEXT_HOP_IPADDR
- For a broadcast interface, you have only the USE_NEXT_HOP_IPADDR option.



Note For the USE_NEXT_HOP_IPADDR option, a field appears in which you *must* enter the required IP address.

Step 23 To continue, click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears.



Note If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Step 24 Click **Add** to join the VPN.

The Join VPN dialog box appears.

Step 25 Check to choose the VPN.

Step 26 Click Join as Hub or Join as Spoke.

Step 27 Click **Done**.

The MPLS Service Request Editor window reappears.

Step 28 Click the **Next** button to associate templates or data files to the service request.



Note

This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 30, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#)

Step 29 When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.

You can define multiple links in this service request, following the instructions outlined in previous steps.

Step 30 To save your work, click **Save**.

The MPLS Service Requests window reappears showing that the MPLS VPN PE-NoCE Service Request is in the Requested state and ready to deploy.



CHAPTER 8

Provisioning Multi-VRFCE PE-CE Links

This chapter describes how to configure MPLS VPN Multi-VRFCE PE-CE links in the IP Solution Center (ISC) provisioning process. It contains the following major sections:

- [MPLS VPN MVRFCE PE-CE Link Overview, page 8-1](#)
- [Creating MPLS VPN MVRFCE PE-CE Service Policies, page 8-4](#)
- [Creating MPLS VPN MVRFCE PE-CE Service Requests, page 8-8](#)
- [Creating an Unmanaged MVRFCE, page 8-19](#)

MPLS VPN MVRFCE PE-CE Link Overview

This section contains the following sections:

- [Network Topology, page 8-2](#)
- [Prerequisite Tasks, 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.

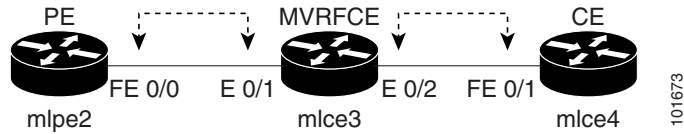
An MVRFCE PE-CE Policy Type is a PE to CE link with three devices:

- PE
- Multi-VRF CE
- CE

This Policy Type has two options:

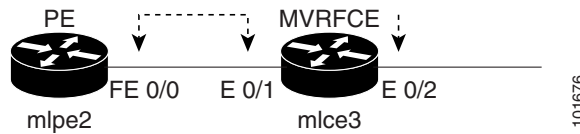
- CE Present *enabled* (One PE with one MVRFCE and one CE; three devices)
- CE Present *disabled* (One PE with one MVRFCE; two devices)

[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.

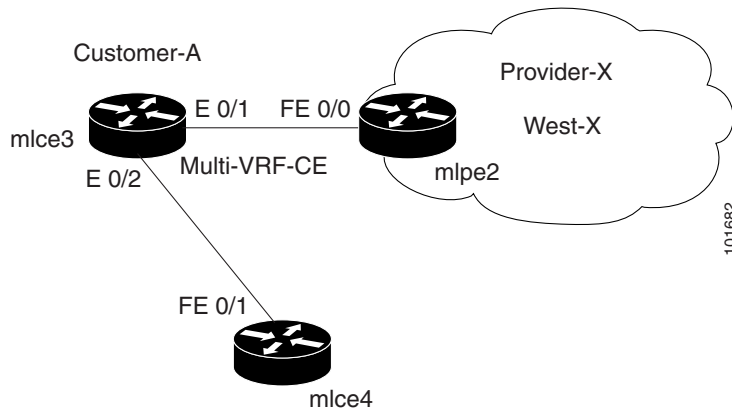
Figure 8-2 shows an example of a PE to MVRFCE link with no CE.

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:

-
- Step 1** Set up a Customer with a Site (see [Creating Customers, Sites, and CPEs, page 2-7](#)).
 - Step 2** Setup a Provider with a Region (see [Creating a Provider, page 2-10](#)).
 - Step 3** Import, create, or discover Devices (see [Creating Devices, page 2-2](#)).
 - Step 4** Create CPE and PE (see [Creating CPEs, page 2-8](#)).
 - Step 5** Collect Configurations (see [Collecting Configurations, page 2-4](#)).
 - Step 6** Create Resource Pools (see [Creating Resource Pools, page 2-15](#)).
 - Step 7** Create CE routing communities (CERC) (see [Creating CE Routing Communities, page 2-32](#)).
 - Step 8** Define a MPLS VPN (see [Creating an MPLS VPN, page 2-22](#)).
-

Defining VPN for MVRFCE PE-CE Links

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, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > VPNs**.
The VPN window appears.
 - Step 2** Click **Create** to create a VPN.
The Create VPN window appears.
 - Step 3** Edit the following attributes:
 - **Name:** Enter the VPN name.
It is recommended not to use special characters (' ` " < > () [] { } / \ & ^ ! ? ~ * % = , . + |) in the VPN name, as this may cause misconfiguration of the VRF name for certain devices, if the VPN name is used to autogenerate a VRF name.
 - **Customer:** Click **Select**.
The Select Customer window appears.
 - Step 4** Choose a Customer and click **Select**.
 - Step 5** Click **Next**.
The VPNs window reappears showing that the VPN Name is associated to the Customer in this new VPN definition.
-

Creating MPLS VPN MVRFCE PE-CE Service Policies

This section contains the following sections:

- [Creating MVRFCE PE-CE Service Policies, page 8-4](#)
- [Creating PE-NoCE Service Policies, page 8-6](#)

Creating MVRFCE PE-CE Service Policies

To create an MVRFCE PE-CE service policy, perform the following steps.



Note

Make sure the Editable check boxes are checked where available, so you can edit these attributes in the service request process.

Step 1 Choose **Service Design > Policies**.

The Policies window appears.

Step 2 From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in [Figure 8-4](#).

Figure 8-4 MPLS Policy Editor - Policy Type

Attribute	Value
Policy Name *	mpls-mvrfce-pe-ce
Policy Owner:	☒ Customer ☐ Provider ☐ Global Policy
Customer *	Select
Policy Type:	☐ Regular: PE-CE ☒ MVRFCE: PE-CE
CE Present:	☒

Note: * - Required Field

Step 3 Edit the following attributes:

- **Policy Name:** Enter the policy name.
- **Policy Owner:** Choose the Policy Owner.
- **Customer:**
 - Click **Select** to specify a customer.
 - The Customer for MPLS Policy window appears.
 - Choose a customer and click **Select**.
- **Policy Type:** Choose the Policy Type. (**MVRFCE: PE-CE**)
- **CE Present:** Check to set CE as present.

Step 4 Click **Next**.

The MPLS Policy Editor - PE Interface window appears, as shown in [Figure 8-5](#).

Figure 8-5 The MPLS Policy Editor - PE Interface

Attribute	Value	Editable
Reset All Attribute Editable Flags:		
		☒
PE Information		
Interface Type:	ANY	
Interface Format:		
Interface Description:		☒
Shutdown Interface:	☐	☒
Use SVT:	☐	☒
Standard UNI Port:	☒	☒
UNI Security Information		
Disable CDP:	☐	☒
Filter BPDUs:	☐	☒
Use Existing ACL Name:	☐	
UNI MAC Addresses:	Edit	☒
UNI Port Security:	☐	☒
MVRFCE PE Facing Information		
Interface Type:	ANY	
Interface Format:		
Interface Description:		☒

- Step 2 of 8 -

< Back Next > Finish Cancel

Step 5 Click **Next**.

The MPLS Policy Editor - Interface window appears.

Step 6 Edit all applicable attributes.

Step 7 Click **Next**.

The MPLS Policy Editor - IP Address Scheme window appears for **PE-MVRFCE**.

Step 8 Edit all applicable attributes.

Step 9 Click **Next**.

Step 10 Another set of MPLS Policy Editor - IP Address Scheme windows appear for **MVRFCE-CE**.

Step 11 Edit all applicable attributes, as above.

Step 12 Click **Next**.

The MPLS Policy Editor - Routing Information window appears for **PE-MVRFCE**.

Step 13 Click **Next** to accept the defaults.

The MPLS Policy Editor - Routing Information window appears for **MVRFCE-CE**.

Step 14 Click **Next** to accept the defaults.

The MPLS Policy Editor - VRF and VPN Membership window appears.

- Step 15** To enable template association for the policy, click the **Next** button in MPLS Policy Editor - VRF and VPN Membership window.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) For additional information about using templates in ISC, also see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). When you have completed setting up templates and data files for the policy per the instructions in the appendix, click **Finish** in the Template Association window to close it.

The Policies window appears.

- Step 16** If you did not enable templates, click **Finish** in the MPLS Policy Editor – VRF and VPN window.

The Policies window reappears showing that the MPLS VPN MVRFCPE PE-CE Service Policy is complete.

Creating PE-NoCE Service Policies

To create a PE-NoCE service policy, perform the following steps.

- Step 1** Choose **Service Design > Policies**.

The Policies window appears.

- Step 2** From the **Create** drop-down list, choose **MPLS Policy**.

The MPLS Policy Editor - Policy Type window appears, as shown in [Figure 8-6](#).

Figure 8-6 MPLS Policy Editor - Policy Type

Attribute	Value
Policy Name *	mpls-mvrfce-pe-noce
Policy Owner:	☒ Customer ☐ Provider ☐ Global Policy
Customer *	CUST-A Select
Policy Type:	☐ Regular: PE-CE ☒ MVRFCPE: PE-CE
CE Present:	☐

Note: * - Required Field

- Step 3** Edit the following attributes:

- **Policy Name:** Enter the policy name.
- **Policy Owner:** Choose the Policy Owner.
- **Customer:**

- Click **Select** to specify a customer.
- The Customer for MPLS Policy window appears.
- Choose a customer and click **Select**.

- **Policy Type:** Choose the Policy Type. (**Regular PE-CE**)
- **CE Present:** Do *not* check to set CE as **not** present (**NoCE**).

Step 4 Click **Next**.

The MPLS Policy Editor - Interface window appears.

Step 5 Click **Next** to accept the defaults.

The MPLS Policy Editor - Interface window appears for **MVRFCE-CE Facing Information**.

Step 6 Click **Next** to accept the defaults.

The MPLS Policy Editor - IP Address Scheme window appears for **PE-MVRFCE-CE Interface Address/Mask**.

- a. Edit the attributes as indicated:
- b. **IP Numbering Scheme:** Choose **IP Numbered** Scheme.
- c. **Automatically Assign IP Address:** To have ISC automatically assign IP Addresses, check the check box.
- d. **IP Address Pool:** Choose the IP Address Pool.

Step 7 Click **Next**.

The MPLS Policy Editor - IP Address Scheme window appears for **MVRFCE-CE Interface Address/Mask**.

- a. Edit the attributes as indicated:
- b. **IP Numbering Scheme:** Choose **IP Numbered** Scheme.
- c. **Automatically Assign IP Address:** To have ISC automatically assign IP Addresses, check the check box.
- d. **IP Address Pool:** Choose the IP Address Pool.

Step 8 Click **Next**.

The MPLS Policy Editor - Routing Information window appears for **PE-MVRFCE Routing Information**.

Step 9 Click **Next** to accept the defaults.

The MPLS Policy Editor - Routing Information window appears for **MVRFCE-CE Routing Information**.

Step 10 Click **Next** to accept the defaults.

The MPLS Policy Editor - VRF and VPN Membership window appears.

Step 11 Click **Add** to join a VPN. The VPN dialog box appears.

Step 12 Click **Join as Hub**, then click **Done**.

The MPLS Policy Editor - VRF and VPN Membership window appears.

Step 13 To enable template association for the policy, click the **Next** button in MPLS Policy Editor - VRF and VPN Membership window.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#) For additional information about using templates in ISC, also see the *Cisco IP Solution Center Infrastructure Reference, 5.1*. When you have completed setting up templates and data files for the policy per the instructions in the appendix, click **Finish** in the Template Association window to close it.

The Policies window appears.

- Step 14** If you did not enable templates, click **Finish** in the MPLS Policy Editor – VRF and VPN window.

The Policies window reappears showing that the MPLS VPN MVRFCE PE-NoCE Service Policy is complete.

Creating MPLS VPN MVRFCE PE-CE Service Requests

This section contains the following sections:

- [Creating MVRFCE PE-CE Service Requests, page 8-8](#)
- [Creating MVRFCE PE-NoCE Service Requests, page 8-14](#)

Creating MVRFCE PE-CE Service Requests

To create an MVRFCE PE-CE service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests window appears.

- Step 2** From the **Create** drop-down list, choose **MPLS Policy**.

The Select MPLS Policy window appears.

- Step 3** Choose the MPLS Policy (**mpls-mvrfce-pe-ce**).

- Step 4** Click **OK**.

The MPLS Service Request Editor window appears.

- Step 5** Click **Add Link**.

The MPLS Service Request Editor window appears, as shown in [Figure 8-7](#).

Figure 8-7 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

Step 6 Click **Select CE**.

The CPE for MPLS VPN Link window appears.

Step 7 Choose the CPE Device and click **Select**.

The MPLS Service Request Editor window appears, as shown in [Figure 8-8](#).

Figure 8-8 MPLS Service Request Editor - Select MVRFCE

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	mlce4	FastEthernet0/1		Select MVRFCE		Select PE		Add	N/A

Step 8 Choose the CE Interface from the drop-down list.

Step 9 Click **Select MVRFCE**.

The MVRFCE for MPLS VPN Link window appears, as shown in [Figure 8-9](#).

Figure 8-9 PE 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.	☐	mlce3.cisco.com	CUST-A	CUST-A-Site-mlce3	MULTI_VRF

Rows per page: Go to page: of 1

Step 10 Choose the MVRFCPE and click **Select**.

The MPLS Service Request Editor window appears, as shown in Figure 8-10.

Figure 8-10 MPLS Service Request Editor - Select MVRFCPE CE Facing Interface

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	MVRFCPE CE Facing Interface	MVRFCPE	MVRFCPE 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 11 Choose the **MVRFCPE CE Facing Interface** from the drop-down list.

Step 12 Choose the **MVRFCPE PE Facing Interface** from the drop-down list.

The MPLS Service Request Editor window appears, as shown in Figure 8-11.

Figure 8-11 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

#	Link ID	CE	CE Interface	MVRFCPE CE Facing Interface	MVRFCPE	MVRFCPE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	☐	0	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Add Details...

Step 13 Click **Add** in the Link Attribute cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in Figure 8-12.

Figure 8-12 MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	mlpe2
Interface Name:	FastEthernet0/0.
Interface Description:	
Shutdown Interface:	☐
Encapsulation:	DOT1Q
VLAN ID *	510 (1-4095)
MVRFCE PE Facing Information	
MVRFCE	mlce3
Interface Name:	Ethernet0/1.
Interface Description:	
Encapsulation:	DOT1Q

Note: * - Required Field

- Step 1 of 7 -

< Back Next > Finish Cancel

PE Information

Step 14 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 15 VLAN ID: Enter the PE VLAN ID.

MVRFCE PE Facing Information

Step 16 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 17 Click **Next**.

The MPLS Link Attribute Editor - Interface window appears, as shown in [Figure 8-13](#).

Figure 8-13 MPLS Link Attribute Editor - Interface

MPLS Link Attribute Editor - Interface

Attribute	Value
MVRFCE CE Facing Information	
MVRFCE	mice3
Interface Name:	Ethernet0/2.
Interface Description:	
Encapsulation:	DOT1Q
VLAN ID *:	530 (1-4095)
CE Information	
CE	mice4
Interface Name:	FastEthernet0/1.
Interface Description:	
Encapsulation:	DOT1Q

Note: * - Required Field

- Step 2 of 7 -

MVRFCE CE Information

Step 18 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 19 VLAN ID: Enter the PE VLAN ID.

MVRFCE PE-Facing Information

Step 20 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 21 Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears for **PE-MVRF-CE interface address/mask**.

Step 22 Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears for **MVRFCE-CE interface address/mask**.

Step 23 Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears for **PE-MVRF-CE routing information**.

Step 24 Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - Routing Information window reappears for **MVRFCE-CE routing information**.

Step 25 Accept the defaults and click **Next**.

The MPLS Link Attribute Editor - VRF and VPN window appears.

Step 26 Click **Add** to join a VPN.

The Select CERCs window appears.

Step 27 Choose a Customer from the drop-down list.

Step 28 Choose a VPN from the drop-down list.

Step 29 Check to choose a VPN from the list.

Step 30 Click **Join As Hub** or **Join As Spoke**.

Step 31 Click **Done**.

The MPLS Link Attribute Editor - VRF and VPN window reappears.

Step 32 Click the **Next** button to associate templates or data files to the service request.



Note

This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 34, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#)

Step 33 When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.

The MPLS Service Request Editor window reappears, as shown in [Figure 8-14](#).

Figure 8-14 MPLS Service Request Editor

#	Link ID	CE	CE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	6	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Edited	Details...

Step 34 Enter the service request description (**mpls-mvrfce-pe-ce**) and click **Save**.

The MPLS Service Requests window reappears showing that the MPLS VPN MVRFCE PE-CE service request is in the Requested state and ready to deploy.

Creating MVRFCE PE-NoCE Service Requests

To create an MVRFCE PE-NoCE service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.
The Service Requests window appears.
- Step 2** From the **Create** drop-down list, choose **MPLS VPN**.
The Select MPLS Policy window appears, as shown in [Figure 8-15](#).

Figure 8-15 Choose MPLS Policy

Select MPLS Policy

Show MPLS policies with matching

Showing 1-5 of 5 records

#	Select	Policy Name	Policy Owner
1.	☐	mpls-mgmt	Customer - CUST-A
2.	☐	mpls-mvrfce-pe-ce	Customer - CUST-A
3.	☒	mpls-mvrfce-pe-noce	Customer - CUST-A
4.	☐	mpls-pe-ce	Customer - CUST-A
5.	☐	mpls-pe-noce	Customer - CUST-A

Rows per page:

101724

- Step 3** Choose the MPLS Policy (**mpls-mvrfce-pe-noce**).
- Step 4** Click **OK**.
The MPLS Service Request Editor window appears.
- Step 5** Click **Add Link**.
The MPLS Service Request Editor window appears, as shown in [Figure 8-16](#).

Figure 8-16 MPLS Service Request Editor - Select MVRFCE

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: mpls-mvrfce-pe-nocce

Description:

Showing 1-1 of 1 records

#	Link ID	CLE	CLE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CLE	Select	Select	Select MVRFCE	Select	Select PE	Select	Add	N/A

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

Step 6 Click **Select MVRFCE**.

The CPE for MPLS VPN Link window appears.

Step 7 Choose a MVRFCE and click **Select**.

The MPLS Service Request Editor window appears, as shown in [Figure 8-17](#).

Step 8 Click **Select MVRFCE**.

Figure 8-17 MPLS Service Request Editor - MVRFCE CE Facing Interface

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: mpls-mvrfce-pe-nocce

Description:

Showing 1-1 of 1 records

#	Link ID	CLE	CLE Interface	MVRFCE CE Facing Interface	MVRFCE	MVRFCE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CLE	Select	Select One	mice3	Select One	Select PE	Select	Add	N/A

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

Step 9 Choose the **MVRFCE CE Facing Interface** from the drop-down list.

Step 10 Choose the **MVRFCE PE Facing Interface** from the drop-down list.

The MPLS Service Request Editor window appears, as shown in [Figure 8-18](#).

Figure 8-18 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

#	☐	Link ID	CLE	CLE Interface	MVRFCPE CE Facing Interface	MVRFCPE	MVRFCPE PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	☐	0	Select CLE		Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Add	Details...

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

101729

Step 11 Click **Add** in the Link Attribute cell.

The MPLS Link Attribute Editor - Interface window appears, as shown in [Figure 8-19](#).

Figure 8-19 MPLS Link Attribute Editor - Interface

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	mlpe2
Interface Name:	FastEthernet0/0.
Interface Description:	
Shutdown Interface:	☐
Encapsulation:	DOT1Q
VLAN ID *	550 (1-4095)
MVRFCPE PE Facing Information	
MVRFCPE	mlce3
Interface Name:	Ethernet0/1.
Interface Description:	
Encapsulation:	DOT1Q

Note: * - Required Field

- Step 1 of 7 -

101730

PE Information

Step 12 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 13 VLAN ID: Enter the PE VLAN ID.

MVRFCE PE Facing Information

Step 14 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 15 Click **Next**.

The MPLS Link Attribute Editor - Interface window appears, as shown in [Figure 8-20](#).

Figure 8-20 MPLS Link Attribute Editor - Interface

Attribute	Value
MVRFCE CE Facing Information	
MVRFCE	mice3
Interface Name:	Ethernet0/2.
Interface Description:	
CE Encapsulation: ⓘ	DOT1Q ▼
VLAN ID *	570 (1-4095)

Note: * - Required Field

- Step 2 of 7 -

< Back Next > Finish Cancel

MVRFCE CE Information

Step 16 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 17 VLAN ID: Enter the PE VLAN ID.

MVRFCE PE Facing Information

Step 18 Encapsulation: Choose the PE Encapsulation from the drop-down list. (**DOT1Q**)

Step 19 Click **Next**.

The MPLS Link Attribute Editor - IP Address Scheme window appears for **PE-MVRF-CE interface address/mask**.

Step 20 Click **Next** to accept the defaults.

The MPLS Link Attribute Editor - IP Address Scheme window appears for **MVRFCE-CE interface address/mask**.

Step 21 Click **Next** to accept the defaults.

The MPLS Link Attribute Editor - Routing Information window reappears for **PE-MVRF-CE routing information**.

Step 22 Click **Next** to accept the defaults.

The MPLS Link Attribute Editor - Routing Information window reappears for **MVRFCE-CE routing information**.

- Step 23** Click **Next** to accept the defaults.
The MPLS Link Attribute Editor - VRF and VPN window appears.
- Step 24** Click **Add** to join a VPN.
The Select CERCs window appears.
- Step 25** Choose a Customer from the drop-down list.
- Step 26** Choose a VPN from the drop-down list.
- Step 27** Check to choose a VPN from the list.
- Step 28** Click **Join As Hub** or **Join As Spoke**.
- Step 29** Click **Done**.
The MPLS Link Attribute Editor - VRF and VPN window reappears.
- Step 30** Click the **Next** button to associate templates or data files to the service request.

**Note**

This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 34, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#)

- Step 31** When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.
The MPLS Service Request Editor window reappears, as shown in [Figure 8-21](#).

Figure 8-21 MPLS Service Request Editor

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: mpls-mvrfce-pe-noce

Description: mpls-mvrfce-pe-noce

Showing 1-1 of 1 records

#	Link ID	CLE	CLE Interface	MVRFC CE Facing Interface	MVRFC	MVRFC PE Facing Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	Select CLE	Ethernet0/2	mlce3	Ethernet0/1	mlpe2	FastEthernet0/0	Edited	Details...	

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

Add Link Delete Link Save Cancel

Step 32 Enter the service request description and click **Save**. (**mpls-mvrfce-pe-noce**)

The MPLS Service Requests window reappears showing that the MPLS VPN MVRFCE PE-NoCE service request is in the Requested state and ready to deploy.

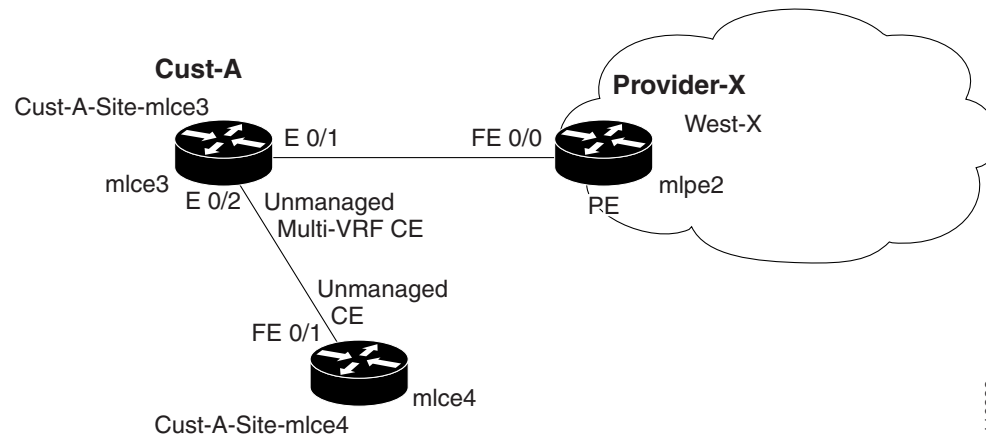
Creating an Unmanaged MVRFCE

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 8-22 shows an overview of a network topology with MPLS VPN MVRFCE PE-CE links.

Figure 8-22 Unmanaged MVRFCE PE-CE Network Topology



The network topology in Figure 8-22 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.



CHAPTER 9

Provisioning Management VPN

This chapter describes how to implement the IP Solutions Center (ISC) Management VPN. It contains the following sections:

- [Overview of the ISC Management Network, page 9-1](#)
- [Provisioning a Management CE in ISC, page 9-8](#)

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:

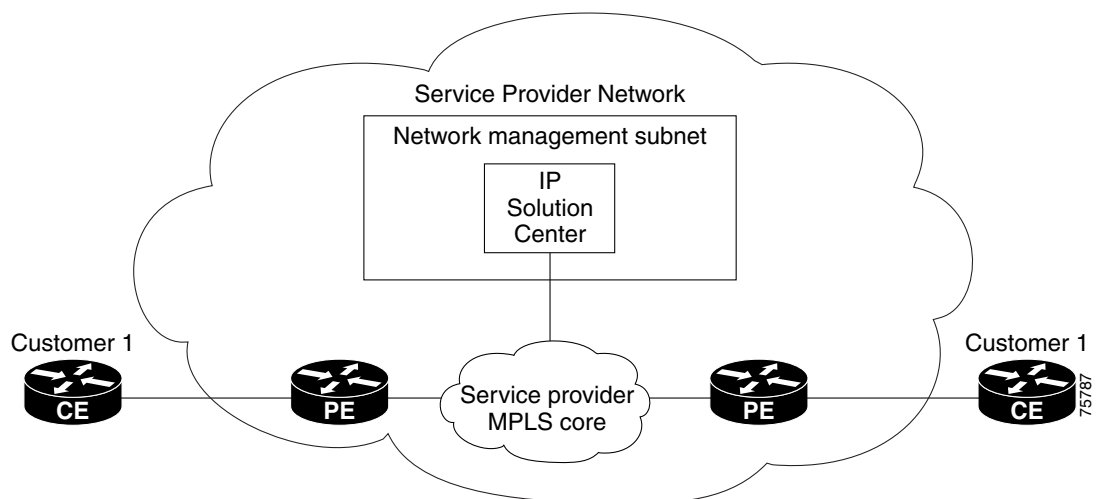
- [Unmanaged Customer Edge Routers, page 9-1](#)
- [Managed Customer Edge Routers, page 9-2](#)
- [Network Management Subnets, page 9-3](#)
- [Implementation Techniques, page 9-4](#)
- [Out-of-Band Technique, page 9-7](#)

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:

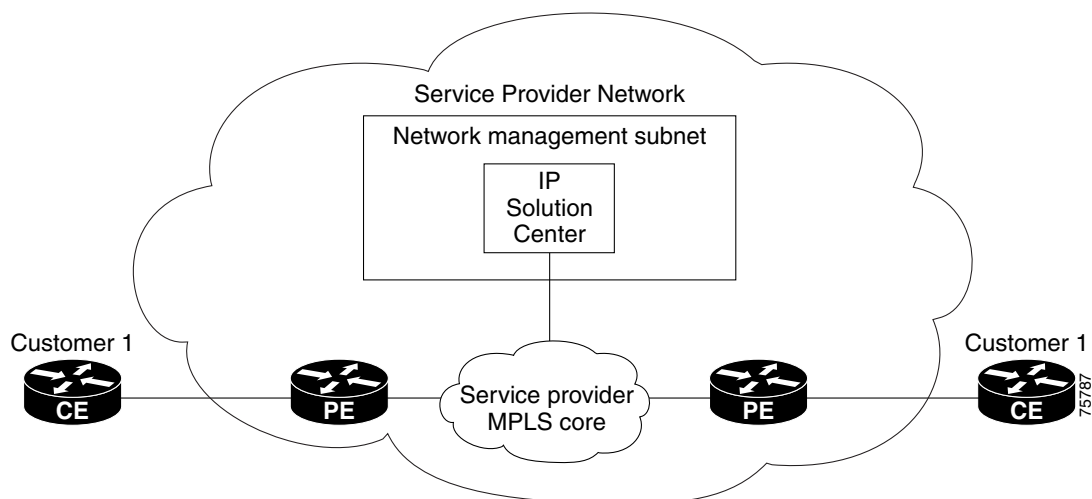
- Managed CEs are within the Service Provider's administrative domain. Thus, some connectivity to the CEs from the Service Provider network is required.
- The Service Provider must administer the following elements on the managed CE:
 - IP addresses
 - Host Name
 - Domain Name server
 - Access data such 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



Note 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.

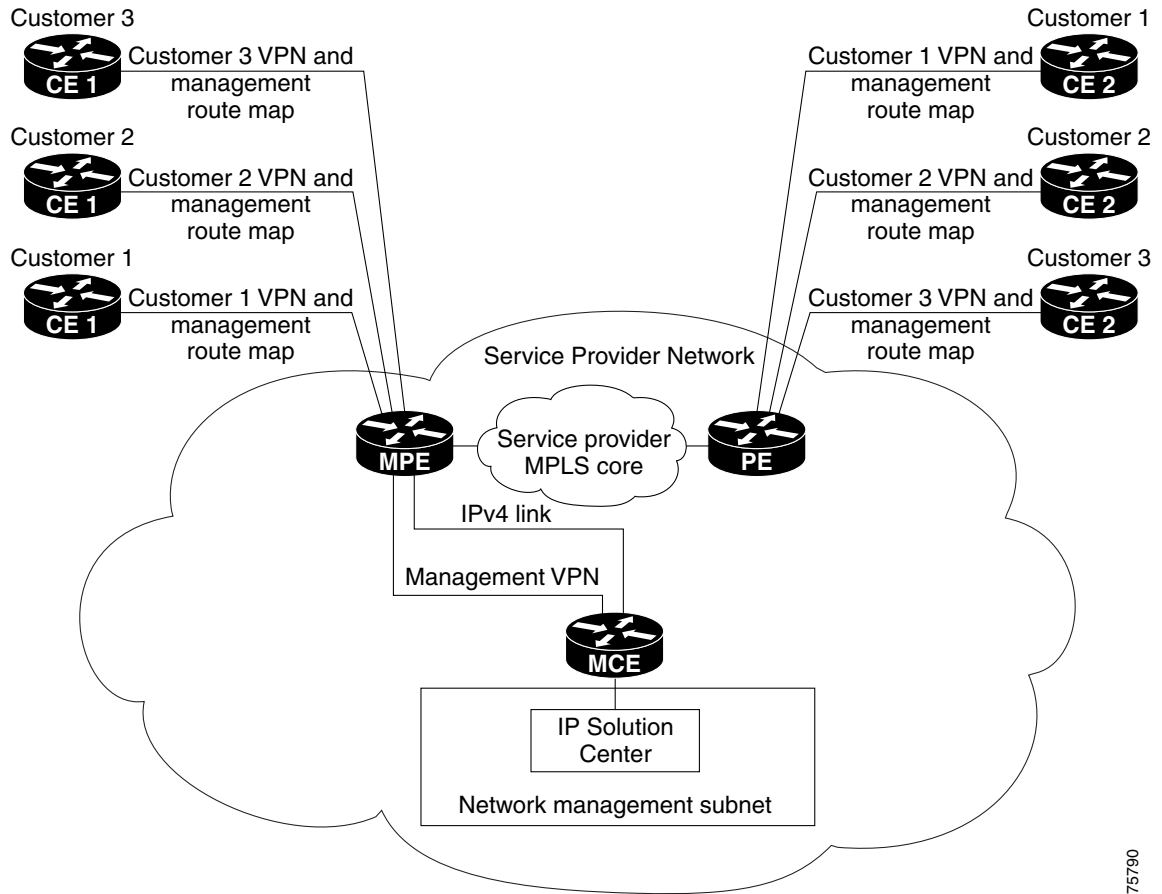
- Out-of-Band Technique

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:

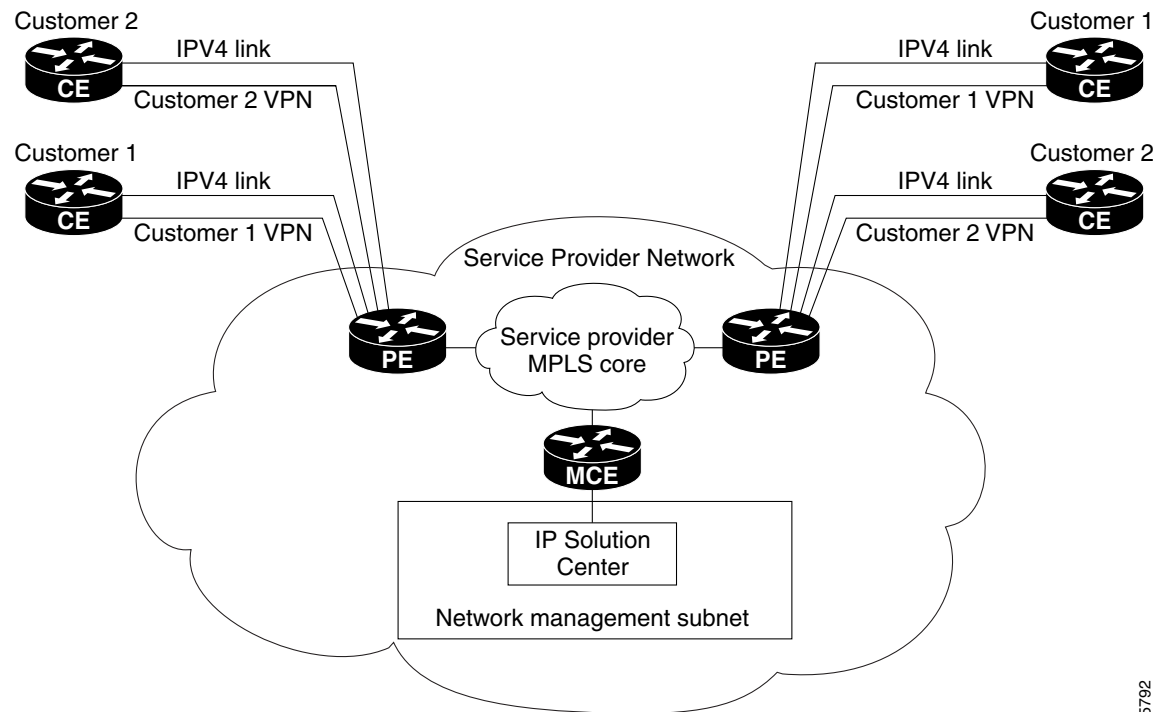
- Provisioning with this method requires only one service request.

- 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.

75792

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 covers the following topics:

- [Defining CE as MCE, page 9-8](#)
- [Creating MCE Service Requests, page 9-10](#)
- [Adding PE-CE Links to Management VPNs, page 9-14](#)

Defining CE as MCE

You configure the MCE by identifying the CE as part of the management LAN in ISC software. To do this, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > CPE Devices**.

The list of CPE devices for all currently defined customers is displayed, as shown in [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

#	☐	Device Name	Customer Name	Site Name	Management Type
1.	☐	mlce1.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
2.	☐	mlce2.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
3.	☐	mlce8.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
4.	☐	mlce9.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
5.	☐	mlsw3.cisco.com	AcmeInc	Acme_SF	Multi-VRF - No SA Agent
6.	☐	mlce12.cisco.com	AcmeInc	Acme_TX	Managed - No SA Agent
7.	☐	mlce13.cisco.com	AcmeInc	Acme_TX	Managed - No SA Agent
8.	☐	mlce3.cisco.com	WidgetsInc	Widgets_SF	Multi-VRF - No SA Agent
9.	☐	mlsw3CE.cisco.com	WidgetsInc	Widgets_SF	Managed - No SA Agent
10.	☐	mlce4.cisco.com	WidgetsInc	Widgets_NY	Managed - No SA Agent

Rows per page: << Page 1, 2 >>

Step 2 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, as shown in [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: Edit

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 >>

Save Cancel

Step 3 **Management Type:** From the drop-down list, set the management type to **Managed—Management LAN**.

Step 4 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, as shown in [Figure 9-7](#).

Figure 9-7 Selected CE Defined as a Management CE

CPE Devices

Show CPEs with Device Name matching Find

Showing 1-5 of 14 records

#	☐	Device Name	Customer Name	Site Name	Management Type
1.	☐	mlce1.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
2.	☐	mlce2.cisco.com	AcmeInc	Acme_NY	Managed - No SA Agent
3.	☐	mlce8.cisco.com	AcmeInc	Acme_SF	Managed - Management LAN
4.	☐	mlce9.cisco.com	AcmeInc	Acme_SF	Managed - No SA Agent
5.	☐	mlsw3.cisco.com	AcmeInc	Acme_SF	Multi-VRF - No SA Agent

Creating MCE Service Requests

To create an MCE service request, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.
The Service Requests dialog box appears.
- 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 window appears.
This window displays the list of all the MPLS service policies that have been defined in ISC.
- Step 4** Choose the policy of choice, then click **OK**.
The MPLS Service Request Editor appears, as shown in [Figure 9-8](#).

Figure 9-8 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

#	☒	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 9-9](#). 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 9-9 Initial Fields Displayed to Define PE-CE Link

#	☐	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

Add Link Delete Link Save Cancel

- Step 6** **CE:** Click **Select CE**.
The Select CPE Device dialog box is displayed, as shown in [Figure 9-10](#).

Figure 9-10 *Selecting the MCE for the MPLS Link*

CPE for MPLS VPN Link

Show CPEs with **Customer Name** matching **Acme*** **Find**

Showing 1-4 of 4 records

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	☐	mlce1.cisco.com	AcmeInc	Acme_NY	MANAGED
2.	☐	mlce2.cisco.com	AcmeInc	Acme_NY	MANAGED
3.	☒	mlce8.cisco.com	AcmeInc	Acme_SF	MANAGED_MGMT_LAN
4.	☐	mlce9.cisco.com	AcmeInc	Acme_SF	MANAGED

Rows per page: **10**

Select **Cancel**

- 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, as shown in [Figure 9-11](#).

Figure 9-11 *CE and CE Interface Fields Defined*

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: **acme_mgmt_pe_ce**

Description:

Showing 1-1 of 1 records

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce8	FastEthernet1/0	Select PE		Add	N/A

Rows per page: **10**

Add Link **Delete Link** **Save** **Cancel**

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, as shown in [Figure 9-12](#).

Figure 9-12 Selecting the PE for the MPLS Link

#	Select	Device Name	Provider Name	Region Name	Role Type
1.	☒	mlpe1.cisco.com	FirstProvider	US	PE_POP
2.	☐	mlpe2.cisco.com	FirstProvider	US	PE_POP
3.	☐	mlpe3.cisco.com	FirstProvider	US	PE_POP
4.	☐	mlpe4.cisco.com	FirstProvider	US	PE_POP

- 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, as shown in [Figure 9-13](#).

Figure 9-13 PE and PE Interface Fields Defined

#	Link ID	CE	CE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	0	mlce8	FastEthernet1/0	mlpe1	FastEthernet1/0	Add	N/A

The Link Attribute **Add** option is now enabled.

- Step 12** In the Link Attribute column, click **Add**.
The MPLS Link Attribute Editor window is displayed, showing the fields for the interface parameters.
The field values displayed in this window 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 5-4.

**Note**

The VLAN ID is shared between the PE and CE, so there is one VLAN ID for both. The Second VLAN ID is an optional attribute that provides a method to match the Q-in-Q second VLAN tag of incoming frames on the PE interface. For usage details about these attributes, see [Notes on the VLAN ID and Second VLAN ID Attributes](#), page 6-10.

- 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, as shown in [Figure 9-14](#).

Figure 9-14 Specifying the MPLS Link IP Address Attributes

MPLS Link Attribute Editor - IP Address Scheme

Attribute	Value
PE-CE Interface Addresses/Mask	
IP Numbering Scheme:	IP Numbered ▾
Extra CE Loopback Required:	☐
Automatically Assign IP Addresses:	☒
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 the IP Address Scheme, page 5-8](#).

- 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, as shown in [Figure 9-15](#).

Figure 9-15 Specifying the MPLS Link Routing Protocol Attributes

MPLS Link Attribute Editor - Ipv4 Routing Information

Attribute	Value
PE-CE Ipv4 Routing Information	
Routing Protocol	BGP ▾
CsC Support:	☐
Redistribute Static (BGP only):	☐
Redistribute Connected (BGP only):	☐
Site of Origin:	☒
Value ⓘ	Select
Neighbor IP Address *	(a.b.c.d)
CE BGP AS ID *	(1-65535)
Neighbor Allow-AS in:	(1-10)
Neighbor AS Override:	☐
Advertise Interval:	(1-600 Seconds)
Max Prefix Number:	(1-2147483647)
Max Prefix Threshold:	(1-100 %)
Max Prefix Warning Only:	☐
Max Prefix Restart:	(1-65535 Minutes)

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 and CE, see [Specifying the Routing Protocol for a Service, page 5-11](#).

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. 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 VRF and VPN Information, page 5-29](#).

- Step 16** Edit any VRF values that need to be modified for this particular link.
- Step 17** Click the **Next** button to associate templates or data files to the service request.

**Note**

This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 34, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#)

- Step 18** When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window. The MPLS Service Request Editor window reappears.
- Step 19** You can add additional links to this service request by choosing **Add Link** and specifying the attributes of the next link in the service.
- Step 20** To save your work in the MPLS Service Request Editor window, click **Save**. You return to the Service Requests window, where the service request is in the Requested state and ready to deploy, as shown in [Figure 9-16](#).

Figure 9-16 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 an asterisk, and a dropdown menu set to 'All'. A 'Find' button is to the right. Below the search bar, it says 'Showing 1-1 of 1 records'. The main part of the window is a table with the following columns: #, Job ID, State, Type, Operation Type, Creator, Customer Name, Policy Name, Last Modified, and Description. There is one row in the table with the following values: 1, 12, REQUESTED, MPLS, ADD, admin, AcmeInc, acme_mgmt_pe_ce, 6/19/03 3:33 PM. Below the table, there is a 'Rows per page:' dropdown set to '10'. At the bottom, there is an 'Auto Refresh:' checkbox which is checked. To the right of the checkbox are several buttons: 'Create', 'Details', 'Edit', 'Deploy', 'Decommission', and 'Purge'. On the far right edge of the window, the number '95376' is visible.

Adding PE-CE Links to Management VPNs

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 do this, perform the following 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.

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.



CHAPTER 10

Provisioning Cable Services

This chapter describes how to provision MPLS VPN cable in IP Solutions Center (ISC). It contains the following sections:

- [Overview of MPLS VPN Cable, page 10-1](#)
- [Provisioning Cable Services in ISC, page 10-5](#)
- [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.

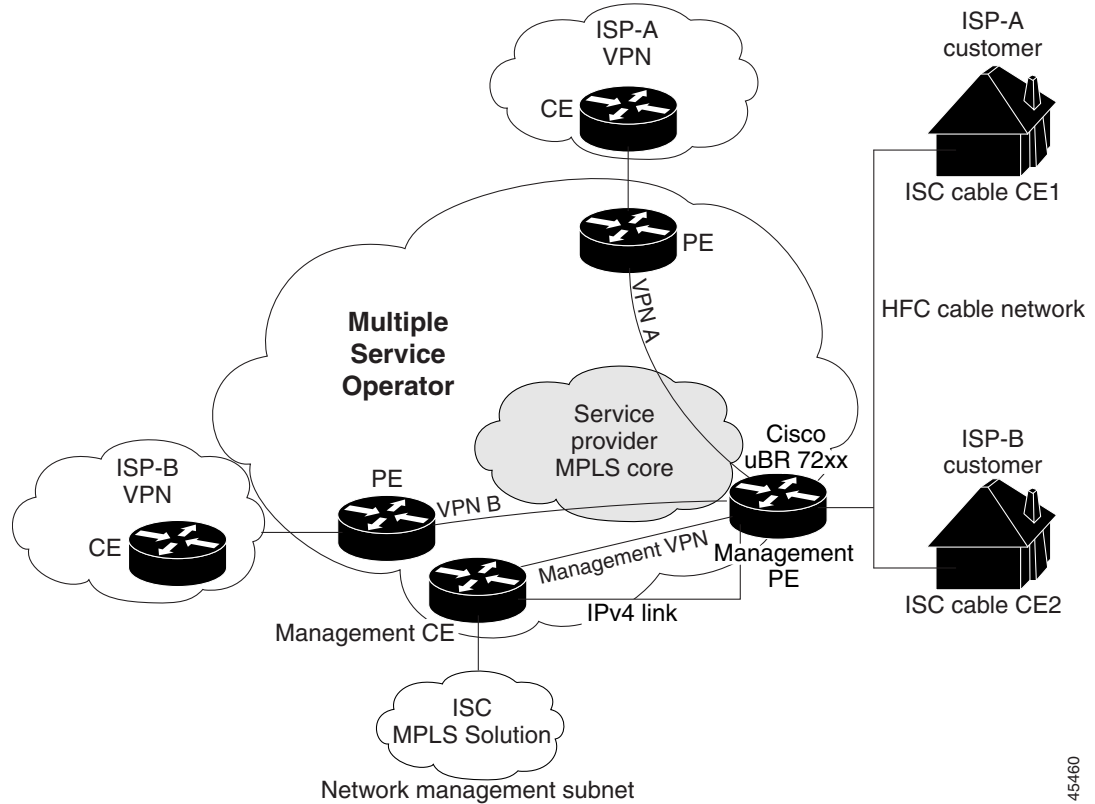
An MPLS VPN assigns a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine the contents of the forwarding table.

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.

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.

Figure 10-1 Example of an MPLS VPN Cable Network

45460

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 host names, routing modifications, privilege levels, and user names 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 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 Cable Link Service Requests, page 10-10](#)

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, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > 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, as shown in [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*

#	Policy Name	Policy Owner
1.	☒ cable	Provider - Provider1
2.	☐ mpls-pe-noc	Customer - Customer1
3.	☐ mpls1	Customer - Customer1

Step 4 Choose the PE-Only policy (**cable** in the example above) policy, and then click **OK**.

The MPLS Service Request Editor appears, as shown in [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

#	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
Showing 0 of 0 records							

Rows per page: 10 Go to page: 1 of 1 [Go](#)

[Add Link](#) [Delete Link](#) [Save](#) [Cancel](#)

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 appears, as shown in [Figure 10-4](#).

Figure 10-4 *Selecting the PE for the MPLS Link*

Select PE Device - Microsoft Internet Explorer

Show PEs with Matching [Find](#)

Showing 1 - 5 of 5 records

#	Device Name	Provider Name	Region Name	Role Type
1.	☒ mipe2	Provider1	West	PE_POP
2.	☐ mipe4	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 [Go](#)

[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, as shown in [Figure 10-5](#).

Figure 10-5 PE and PE Interface Fields Defined

MPLS Service Request Editor

Job ID: SR ID: SR State:

Policy: cable

Customer: [Select Customer](#)

Description:

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:

Go to page: of 1 [Go](#)

[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, as shown in [Figure 10-6](#).

Figure 10-6 Specifying the MPLS Link Interface Attributes

MPLS Link Attribute Editor - Interface

Attribute	Value
PE Information	
PE	enpe1
Interface Name:	Cable0/1.
Interface Description:	cable maintenance
Shutdown Interface:	☒
Cable Maintenance Interface:	☒
Cable Helper Addresses:	Edit

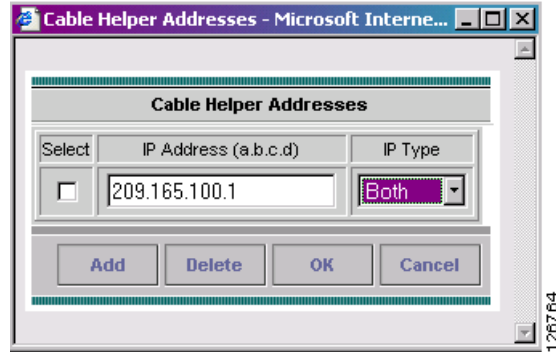
Step 10 Enter a subinterface name in the Interface Description field.

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

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.

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.

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. The field values displayed in this dialog box reflect the values specified in the service policy associated with this service.



Note If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

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.

Step 20 Click the **Next** button to associate templates or data files to the service request.



Note This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 34, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#)

Step 21 When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.



Note You can define multiple links in this service request.

Step 22 To save your work on this service request, click **Save**.

The MPLS Service Requests window reappears showing that the service request is in the Requested state and ready to deploy.

Creating Cable Link Service Requests

To create a cable link service request, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.

The Service Requests dialog box appears.

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, as shown in [Figure 10-8](#). This dialog box displays the list of all the MPLS service policies that have been defined in ISC.

Figure 10-8 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. ☐	cable	Provider - Provider1
2. ☒	cable1	Global
3. ☐	mpls-pe-noce	Customer - Customer1
4. ☐	mpls1	Customer - Customer1

Rows per page:

126744

Step 4 Choose the policy of choice, then click **OK**.

The MPLS Service Request Editor appears.

Step 5 Click **Add Link**.

The MPLS Service Request Editor now displays a set of fields, as shown in [Figure 10-9](#). Note that in the PE column, the **Select PE** option is now enabled.

Figure 10-9 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

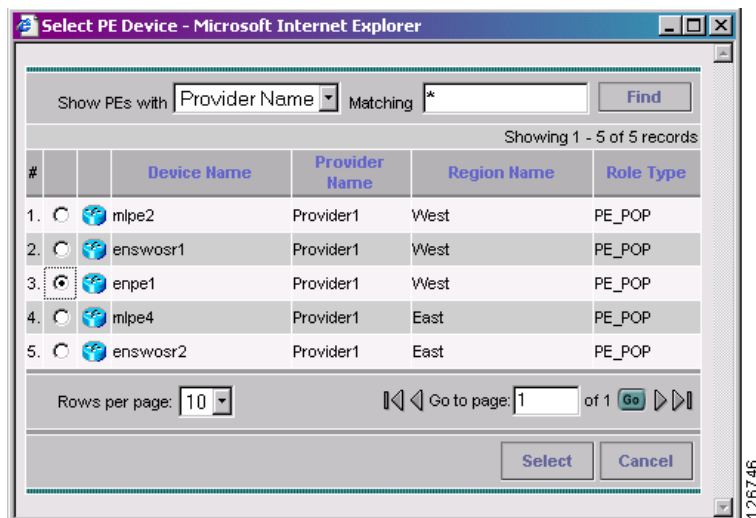
#	☐	Link ID	CLE	CLE Interface	PE	PE Interface	Link Attribute	Logical Link
1.	☐	0	Select CLE		Select PE		Add	N/A

Rows per page:

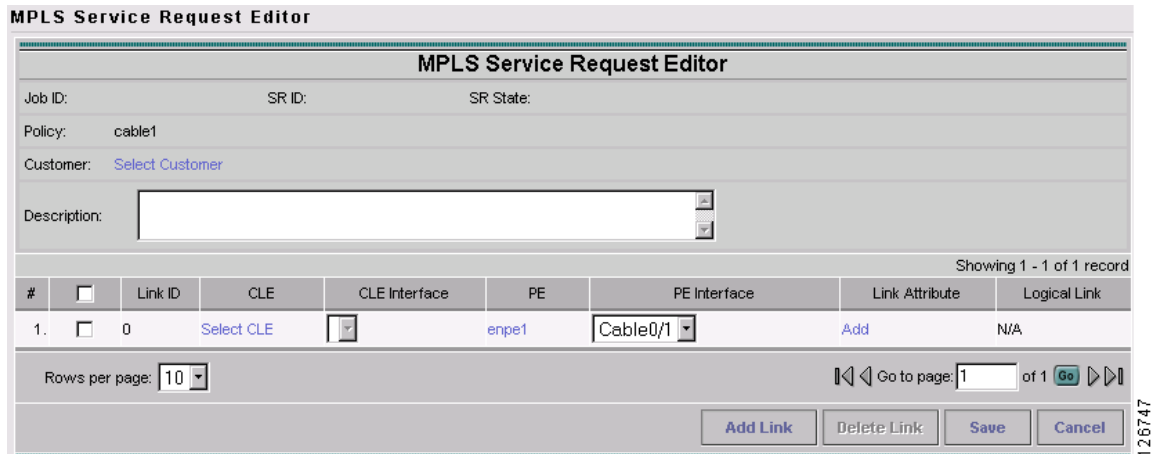
126745

Step 6 **PE:** Click **Select PE**.

The Select PE Device dialog box is displayed, as shown in [Figure 10-10](#).

Figure 10-10 Selecting the PE for the MPLS Link

- 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, as shown in Figure 10-11.

Figure 10-11 PE and PE Interface Fields Defined

Note that 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, as shown in Figure 10-12.

Figure 10-12 Specifying the MPLS Link Interface Attributes

Attribute	Value
PE Information	
PE	enpe1
Interface Name *	Cable0/1
Interface Description:	for ISP_1
Shutdown Interface:	☐
Cable Maintenance Interface:	☐
Cable Helper Addresses:	Edit
Secondary Addresses:	Edit

Note: * - Required Field



Note Do not check the box for Cable Maintenance Interface.

Step 10 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 11 Click **Add**.

The Cable Helper Addresses window appears as shown in [Figure 10-13](#).

Figure 10-13 Cable Helper Addresses

Select	IP Address (a.b.c.d)	IP Type
☐	209.165.200.10	Modem

[Add](#) [Delete](#) [OK](#) [Cancel](#)

Step 12 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.)

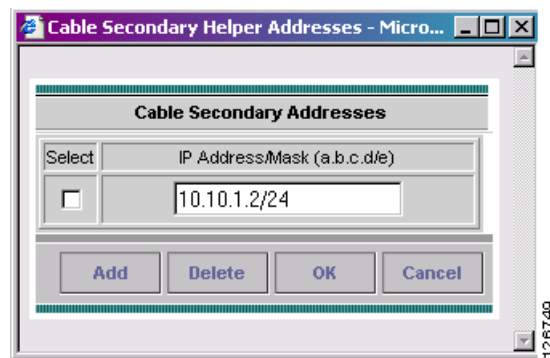
Step 13 Click **OK**.

The MPLS Link Attribute Editor reappears.

Step 14 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 10-14 Cable Secondary Addresses



Step 15 Enter an IP address in the IP address/Mask field and click **OK**.

The MPLS Link Attribute Editor reappears.

Step 16 Click **Next**.

Step 17 The MPLS Link Attribute Editor for the IP Address Scheme appears.

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.

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. The field values displayed in this dialog box reflect the values specified in the service policy associated with this service.



Note

If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

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 10-15 Choose CERCs

Select CERCs - Microsoft Internet Explorer

Customer: VPN:

Showing 1-1 of 1 records

#	☐	Customer	VPN	Provider	CERC	Topology
1.	☒	ISP_1	isp_1	Provider_A	Default	Hub and Spoke

Rows per page:

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.

Step 24 Edit any VRF and VPN values that must be modified for this particular link.

Step 25 Click the **Next** button to associate templates or data files to the service request.



Note

This step assumes the policy on which the service request is based has template association enabled. If not, there will be no **Next** button visible in the GUI. In that case, click **Finish** and return to the MPLS Service Request Editor window and proceed with Step 34, below.

The MPLS Link Attribute Editor - Template Association window appears. In this window, you can associate templates and data files with a device by clicking the **Add** button in Template/Data File column for the device. When you click the **Add** button, the Add/Remove Templates window appears. For instructions about associating templates with service requests and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files.”](#)

Step 26 When you have completed setting up templates and data files for any device(s), click **Finish** in the Template Association window to close it and return to the MPLS Service Request Editor window.



Note

You can define multiple links in this service request.

Step 27 To save your work on this service request, click **Save**.

The MPLS Service Requests window reappears showing that the service request is in the Requested state and ready to deploy.



CHAPTER 11

Provisioning Carrier Supporting Carrier

This chapter describes how to configure the carrier supporting carrier (CSC) feature using the IP Solution Center (ISC) provisioning process. It contains the following sections:

- [Carrier Supporting Carrier Overview, page 11-1](#)
- [Defining CSC Service Policies, page 11-5](#)
- [Provisioning CSC Service Requests, 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

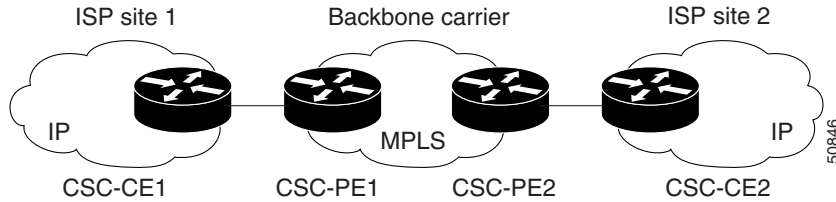
This documentation describes both types of customer carrier.

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 ISP Customer Carrier

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 an ISP Customer Carrier*

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:

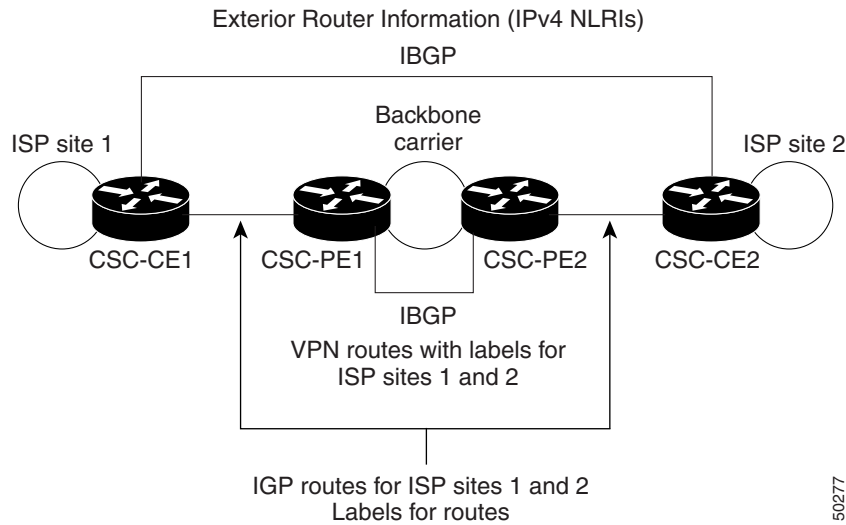
- Internal routes go to any of the routers within the ISP.
- External routes go to the Internet.

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

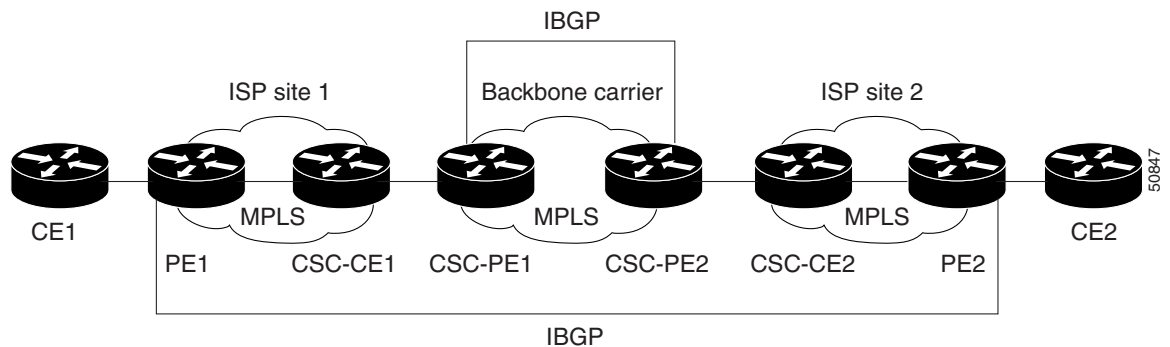
Backbone Network with BGP/MPLS VPN Service Provider Customer Carrier

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.

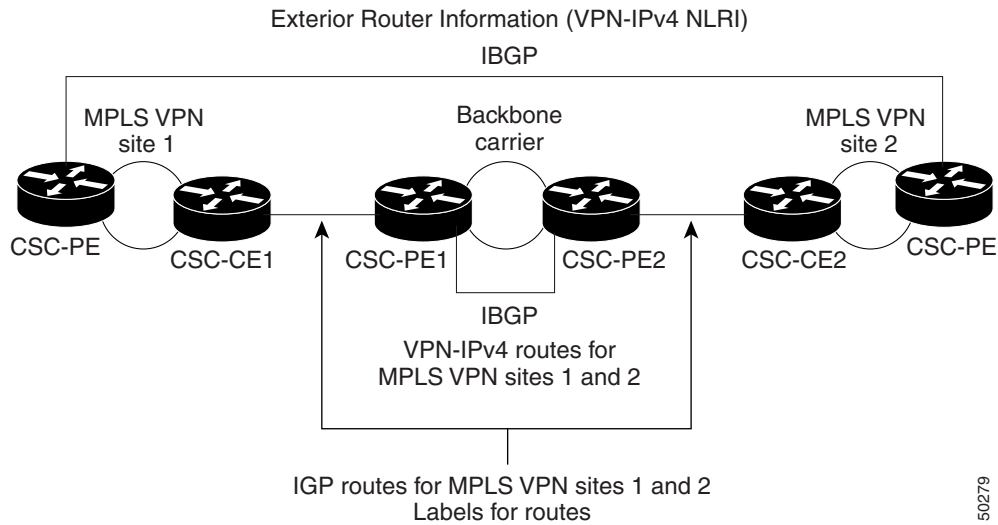
Figure 11-3 Carrier Supporting Carrier Network with a Customer Carrier Who Is an MPLS VPN Provider



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 CSC Service Policies

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 - Ipv4 Routing Information	
Attribute	Value
PE-CE Ipv4 Routing Information	
Routing Protocol	RIP
CsC Support:	☒
Give Only Default Routes to CE:	☐
Redistribute Static (BGP only):	☐
Redistribute Connected (BGP only):	☐
RIP Metrics (BGP only):	(1-16)
Redistributed Protocols on PE:	Edit
Redistributed Protocols on CE:	Edit

When CSC Support is checked, the CSC functionality is enabled to the MPLS VPN service.

Provisioning CSC Service Requests

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 - Ipv4 Routing Information

Attribute	Value
PE-CE Ipv4 Routing Information	
Routing Protocol	RIP
CsC Support:	☒
Give Only Default Routes to CE:	☐
Redistribute Static (BGP only):	☐
Redistribute Connected (BGP only):	☒
RIP Metrics (BGP only):	(1-16)
Redistributed Protocols on PE:	Edit
Redistributed Protocols on CE:	Edit

Note: * - Required Field

When CSC Support is checked, the CSC functionality is enabled for the MPLS VPN service.



CHAPTER 12

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. It contains the following sections:

- [NPC Ring Topology, page 12-1](#)
- [Ethernet-To-The-Home \(ETTH\), 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:

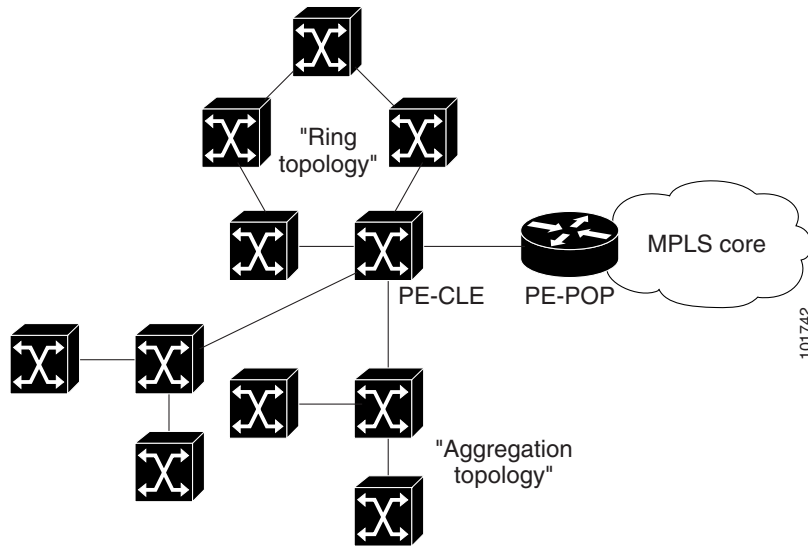
- [Ring Topology Overview, page 12-1](#)
- [Creating Ring of Three PE-CLEs, page 12-2](#)
- [Configuring NPC Ring Topology, page 12-5](#)

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”)

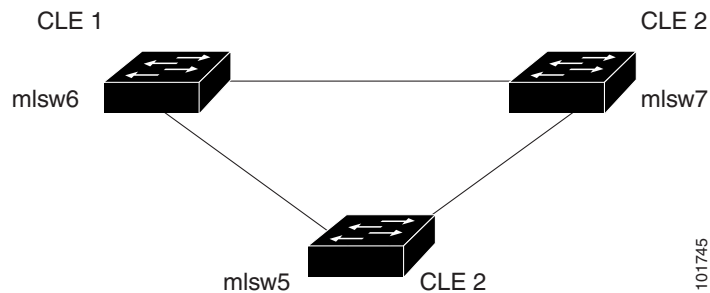
[Figure 12-1](#) shows an example of these two basic L2 access topologies.

Figure 12-1 L2 Access Topologies

Creating Ring of Three PE-CLEs

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 of three PE-CLEs, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
 - Step 2** 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 3 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.	☐ Select source device	Select source interface	Select destination device	Select destination interface
2.	☐ Select source device	Select source interface	Select destination device	Select destination interface
3.	☐ Select source device	Select source interface	Select destination device	Select destination interface

Step 4 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.	☒	mlsw6.cisco.com	PROVIDER-X	NORTH-X	PE_CLE

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

Step 5 To search for a specific CLE, enter the *source device* in the **matching** dialog-box and click **Find**.

Step 6 Choose the CLE and click **Select**.

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

Figure 12-6 Create Ring

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	mlce4	FastEthernet0/1	Ethernet0/2	mlce3	Select One	Select PE		Add	N/A

Rows per page: 10

Go to page: 1 of 1

Add Link

Delete Link

Save

Cancel

Step 7 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 8 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

Create a Named Physical Circuit

#	☐	Device	Incoming Interface	Outgoing Interface	Ring
1.	☒	mlce14		Select outgoing interface	
2.	☐	mlpe4	Select incoming interface		

Insert Device

Insert Ring

Add Device

Add Ring

Delete

Save

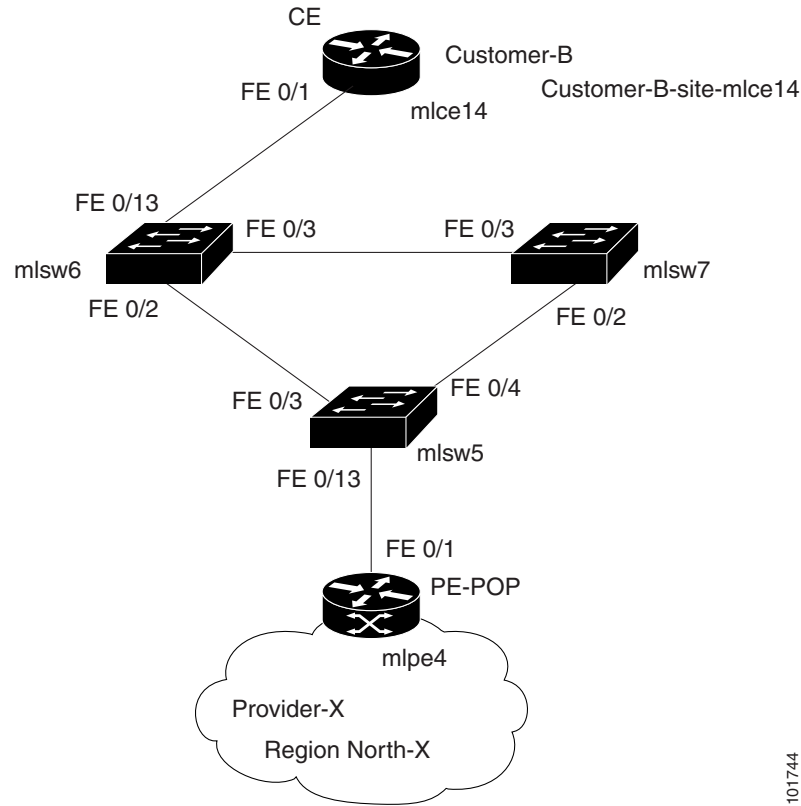
Cancel

Proceed to [Configuring NPC Ring Topology, page 12-5](#).

Configuring NPC Ring Topology

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

Figure 12-8 *The Ring Topology*



To configure end-to-end connectivity (CE > Ring (PE-CLE) > PE), perform the following steps.

- Step 1** Choose **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*

Named Physical Circuits

Show NPCs where Matching

Showing 0 of 0 records

#	Source Device	Source Interface	Destination Device	Destination Interface	Name

Rows per page: Go to page: of 1

116324

Step 2 Click **Create**.

The Create a Named Physical Circuit window appears, as shown in [Figure 12-10](#).

Figure 12-10 *Create a Named Physical Circuit*

Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring

116325

Step 3 Click **Add Device**.

The Select Devices window appears.

Step 4 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*

Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	☒ mlce14			

116330

Step 5 Click **Add Device**.

The Select Devices window appears, as shown in [Figure 12-12](#).

Figure 12-12 Choose Devices

Showing 1 - 7 of 7 records

#	Device Name	Provider Name	Region Name	PE Role Type
1.	☐ mlpe1	Provider-X	West-X	PE_POP
2.	☐ mlpe2	Provider-X	West-X	PE_POP
3.	☐ mlpe3	Provider-X	West-X	PE_POP
4.	☒ mlpe4	Provider-X	West-X	PE_POP
5.	☐ mlsw5	Provider-X	North-X	PE_CLE
6.	☐ mlsw6	Provider-X	North-X	PE_CLE
7.	☐ mlsw7	Provider-X	North-X	PE_CLE

Rows per page: 50 Go to page: 1 of 1

Select Cancel

Step 6 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

Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	☒ mlce14		Select outgoing interface	
2.	☐ mlpe4	Select incoming interface		

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

Step 7 Click **Insert Ring**.

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

Figure 12-14 Show NPC Rings

Showing 1 - 1 of 1 record

#	Ring Name
1.	1-m1sw6-FastEthernet0/3

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

Select Cancel

Step 8 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.	☐ mlce14		Select outgoing interface	
2.	☒ Select device	Select incoming interface		1-mlsw6-FastEthernet0/3
3.	☐ Select device		Select outgoing interface	1-mlsw6-FastEthernet0/3
4.	☐ mlpe4	Select incoming interface		

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

116334

Step 9 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

Show **PE** devices where **Device Name** Matching * Find

Showing 1 - 3 of 3 records

#	Device Name	Provider Name	Region Name	PE Role Type
1.	☐ mlsw5	Provider-X	North-X	PE_CLE
2.	☒ mlsw6	Provider-X	North-X	PE_CLE
3.	☐ mlsw7	Provider-X	North-X	PE_CLE

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

Select Cancel

116335

Step 10 Choose a PE-CLE and click **Select**.

The Create a Named Physical Circuit window appears.

Step 11 Choose the incoming and outgoing interfaces for the CE, CLE, and PE until complete.

Step 12 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

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	☒ mlce14		FastEthernet0/1	
2.	☐ mlsw6	FastEthernet0/13		1-mlsw6-FastEthernet0/3
3.	☐ mlsw5		FastEthernet0/13	1-mlsw6-FastEthernet0/3
4.	☐ mlpe4	FastEthernet0/1		

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

116337

Step 13 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*

#	☐	Source Device	Source Interface	Destination Device	Destination Interface	Name
1.	☐	mlsw5	FastEthernet0/13	mlpe4	FastEthernet0/1	1-(mlsw5-FastEthernet0/13)<==>(mlpe4-FastEthernet0/1)
2.	☐	mlsw6		mlpe4	FastEthernet0/1	2-(mlsw6-)<==>(mlpe4-FastEthernet0/1)
3.	☐	mlsw7		mlpe4	FastEthernet0/1	3-(mlsw7-)<==>(mlpe4-FastEthernet0/1)
4.	☐	mlce14	FastEthernet0/1	mlpe4	FastEthernet0/1	4-(mlce14-FastEthernet0/1)<==>(mlpe4-FastEthernet0/1)

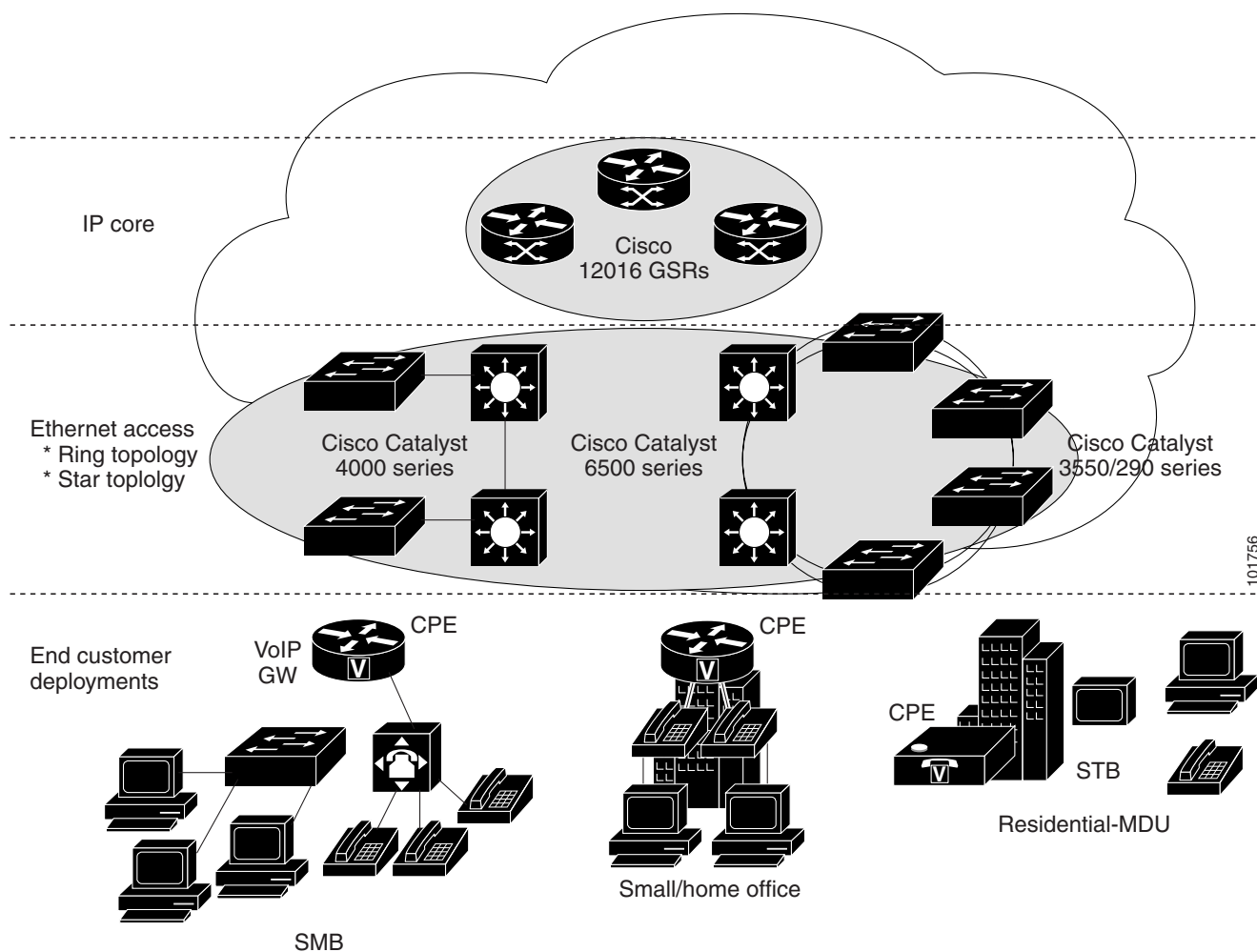
Ethernet-To-The-Home (ETTH)

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

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 subfeatures:

- [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 coming 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.

Creating an ETTH Policy

To configure a policy to support ETTH, perform the following steps.

- Step 1** Choose **Service Design > Policies**.
- Step 2** From the Policies window, choose a Service Policy and click **Edit**.
- Step 3** 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
Reset all Attribute editable flags:		☒
PE Information		
Interface Type:	ANY	
Interface Format:		
Interface Description:		☒
Shutdown Interface:	☐	☒
Auto-Pick VLAN ID:	☐	☒
Link Speed:	None	☒
Link Duplex:	None	☒
ETTH Support:	☒	☒
CE Information		
Interface Type:	ANY	
Interface Format:		
Interface Description:		☒

- Step 2 of 5 -

< Back Next > Finish Cancel

- Step 4** To enable ETTH, check 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

ETTH Support:	☒	☒
UNI Information		
Private VLAN/Protected Port:	☒	☒
IGMP Snooping with MVR:	☒	☒
CE Information		

- Step 5** To enable Private VLAN or Protected Port, check the **Private VLAN/Protected Port** check box.
- Step 6** To enable IGMP Snooping with MVR, check 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:	☒	☒
IGMP Snooping with MVR:	☒	☒
Mode:	☒ Compatible ☐ Dynamic	☒
Query Time:	(1-100)	☒
Immediate:	☐	☒

101747

Step 7 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 8 Complete the standard steps and click **Save**.

Creating a Service Request for ETTH

To create a service request for ETTH, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.

Step 2 From the Service Requests window, choose a Service Request and click **Edit**.

Step 3 From the MPLS Service Request Editor window, click the **Link Attribute** link.

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
PE Information	
PE	pe1
Interface Name:	Ethernet4/2. (1-4294967295)
Interface Description:	
Shutdown Interface:	☐
PE Encapsulation: ⓘ	DOT1Q v
VLAN ID *:	(1-4094)
Auto-Pick VLAN ID:	☐
Second VLAN ID: ⓘ	(1-4094)
Use SVI:	☐
ETTH Support:	☒
Standard UNI Port:	☐
UNI Information	
Shared VLAN:	☐
Private VLAN/Protected Port:	☒
Secondary VLAN ID: ⓘ	(1-4094)
IGMP Snooping with MVR:	☒
Mode:	☒ Compatible ☐ Dynamic
Query Time:	(1-100)
Multicast IP Address:	Edit
Multicast VLAN ID:	(1-4094)
Immediate:	☐

Note: * - Required Field

- Step 1 of 3 -

< Back Next > Finish Cancel

Step 4 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 5](#).
- **Multicast VLAN ID**—Enter a *VLAN ID* for the Multicast VLAN.

Step 5 Click **Edit**.

The Multicast IP Addresses dialog box appears, as shown in [Figure 12-24](#).

Figure 12-24 Multicast IP Addresses

Select	Multicast IP Address (a.b.c.d)	Counter (1 - 256)
☐	224.3.3.1	12

Buttons: Add, Delete, OK, Cancel

101751

Step 6 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 7 Click **OK**.

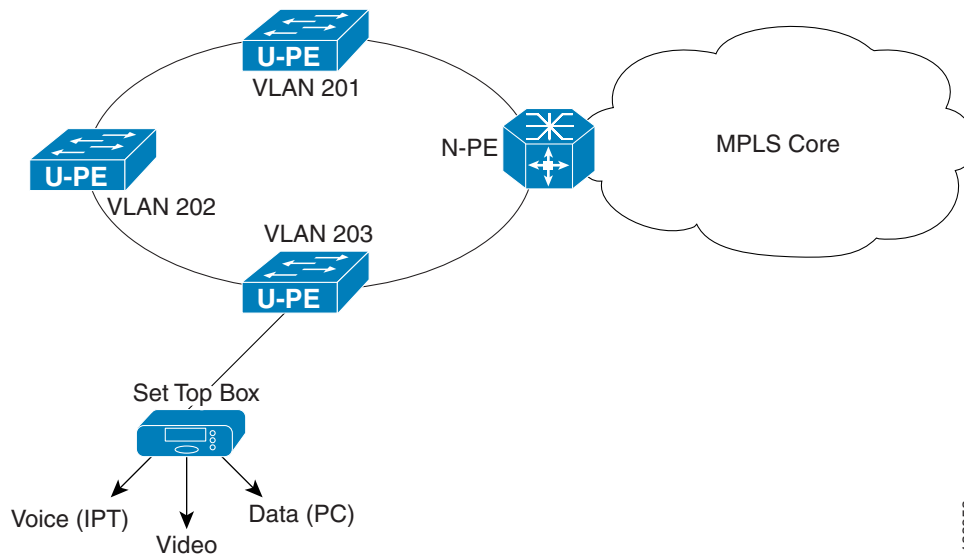
Step 8 Complete the standard steps for creating a service request, and click **Save**.

The MPLS Service Requests window reappears showing that the service request is in the Requested state and ready to deploy.

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, as shown in [Figure 12-25](#).

Figure 12-25 Residential Services



138953

Creating a Policy for Residential Services Over Shared VLAN

A special policy must be created by enabling Shared VLAN. To do this, perform the following steps.

- Step 1** Choose **Service Design > Policies**.
- Step 2** From the Policies window, click **Create > MPLS Policy**.
The Policy Type window appears, as shown in [Figure 12-26](#).

Figure 12-26 Policy Type

MPLS Policy Editor - Policy Type

Attribute	Value
Policy Name *	mlReserv1
Policy Owner:	☐ Customer ☐ Provider ☒ Global Policy
Policy Type:	☒ Regular: PE-CE ☐ MVRFC: PE-CE
CE Present:	☐

Note: * - Required Field

138954

- Step 3** In the Policy Name field, enter a policy name.
- Step 4** Under Policy Owner, click the **Global Policy** radio button.
- Step 5** Under Policy Type accept **Regular: PE-CE**.

- Step 6** Under CE Present, uncheck the check box, then click **Next**.
The MPLS Policy Editor - Interface window appears, as shown in [Figure 12-27](#).

Figure 12-27 Interface Settings

MPLS Policy Editor - Interface

Attribute	Value	Editable
Reset All Attribute Editable Flags:		☒
PE Information		
Interface Type:	ANY	
Interface Format:		
Interface Description:		☒
Shutdown Interface:	☐	☒
Auto-Pick VLAN ID:	☐	☒
Use SVI:	☒	☒
Link Speed:	None	☒
Link Duplex:	None	☒
ETTH Support:	☒	☒
Standard UNI Port:	☒	☒
UNI Information		
Shared VLAN:	☒	☐
Private VLAN/Protected Port:	☒	☒
IGMP Snooping with MVR:	☐	☒
UNI Security Information		
Disable CDP:	☐	☒
Filter BPDU:	☐	☒
Use Existing ACL Name:	☐	
UNI MAC Addresses:	Edit	☒
UNI Port Security:	☐	☒

138955

- Step 7** Check the **Use SVI:** check box, then wait for the window to refresh.
- Step 8** Check the **ETTH Support:** check box, then wait for the window to refresh.
- Step 9** Check the **Standard UNI Port:** check box, then wait for the window to refresh.
- Step 10** Check the **Shared VLAN:** check box, then wait for the window 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 11** Check the **Private VLAN/Protected Port:** check box, wait for the window to refresh, then click **Next**.
- Step 12** In the IP Address Scheme window, you can continue by clicking **Next**.
- Step 13** In the Routing Information window, you can continue by clicking **Next**.
- Step 14** In the VRF and VPN Member window, you can continue by clicking **Next** to associate templates, or else finish creating this policy by clicking **Finish**.

Creating a Service Request for Residential Services Over Shared VLAN

To create the service request, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Service Requests**.
 - Step 2** From the Service Requests window, click **Create > MPLS VPN**.
The Select MPLS Policy window appears.
 - Step 3** Choose the policy you configured for Shared VLAN Residential Services, then click **OK**. The MPLS Service Request Editor window appears.
 - Step 4** In the MPLS Service Request Editor window, click **Add Link**, then wait for the window to refresh.
 - Step 5** Click the active field **Select U-PE**.
 - Step 6** Choose a PE device, then click **Select**.
 - Step 7** From the active drop-down list, choose an interface, then wait for the window to refresh.
 - Step 8** Under Link Attributes column, click the active **Add** field.
The Interface window appears, as shown in [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
PE Information	
PE	pe1
Interface Name:	Ethernet4/2. (1-4294967295)
Interface Description:	
Shutdown Interface:	☐
PE Encapsulation: ⓘ	DOT1Q v
VLAN ID *	(1-4094)
Auto-Pick VLAN ID:	☐
Second VLAN ID: ⓘ	(1-4094)
Use SVI:	☒
ETTH Support:	☒
Standard UNI Port:	☒
UNI Information	
Shared VLAN:	☒
Private VLAN/Protected Port:	☒
Secondary VLAN ID: ⓘ	(1-4094)
IGMP Snooping with MVR:	☐
UNI Security Information	
Disable CDP:	☐
Filter BPDU:	☐
Use Existing ACL Name:	☐
UNI MAC Addresses:	Edit
UNI Port Security:	☐

Note: * - Required Field

211711

Step 9 Enter a valid **VLAN ID** value, then click **Next**. The IP Address Scheme window appears.

Step 10 Enter valid values for each required field, then click **Next**.

Step 11 In the Routing Information window, check any applicable items, then click **Next**.

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

**Note**

If you want to set the VRF and VPN attributes via a previously defined VRF object, check the **Use VRF Object** check box. For more information on this feature, see [Chapter 3, “Independent VRF Management.”](#) That chapter describes how to use independent VRF objects in MPLS VPN service policies and service requests.

Step 13 Under VPN Selection (required), click **Add**.

Step 14 From the CERC window, choose the desired PE VPN Membership, then click **Done**.

Step 15 Back in the VRF and VPN window, click **Finish**.

**Note**

If the policy on which the service request is based has template association enabled, a **Next** button is visible in the GUI. Click the **Next** button to add templates and data files to the devices defined in the service request. For instructions about associating templates with service requests, see [Appendix B, “Working with Templates and Data Files.”](#)

When you are finished setting the attributes for the service policy, the MPLS Service Request Editor window appears.

Step 16 Click **Save**.

The MPLS Service Requests window reappears showing that the service request is in the Requested state and ready to deploy.



CHAPTER 13

Spanning Multiple Autonomous Systems

This chapter describes how to configure spanning multiple autonomous systems using the IP Solution Center (ISC) provisioning process. It contains the following sections:

- [Overview, page 13-1](#)
- [Routing Between Autonomous Systems, page 13-3](#)
- [Routing Between Subautonomous Systems in a Confederation, page 13-8](#)
- [Using ISC to Span Multiple Autonomous Systems, page 13-9](#)
- [Using Templates to Support Inter-Autonomous System Solutions, page 13-11](#)

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 13-3](#) 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 subautonomous 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.

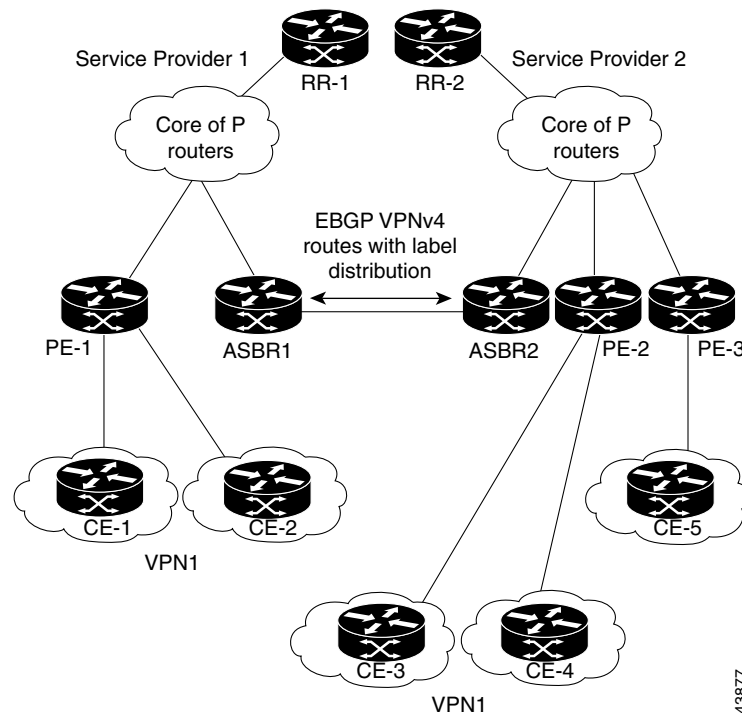
- Allows confederations to optimize IBGP meshing

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 subautonomous 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 subautonomous 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.

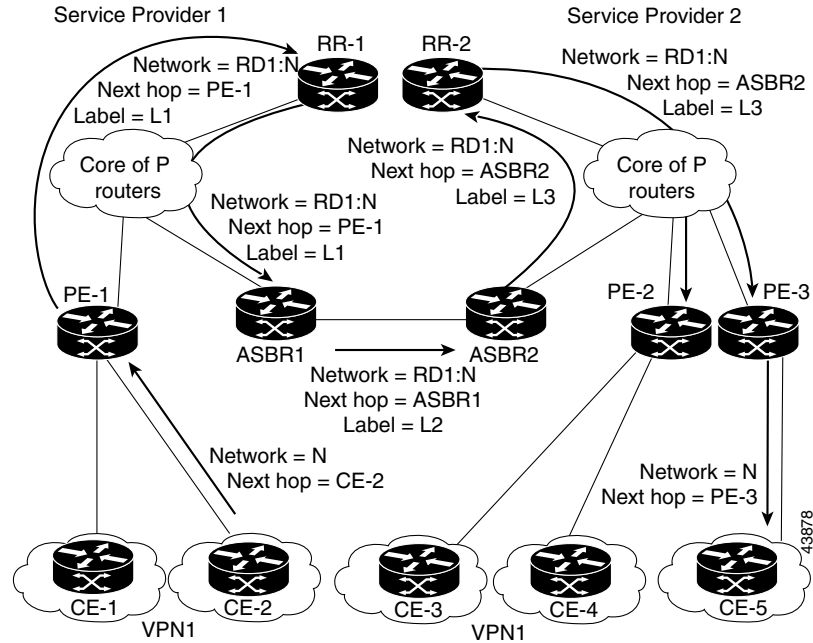
Figure 13-2 *Exchanging Routes and Labels Between Two Autonomous Systems*

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 configured to change the next hop address.

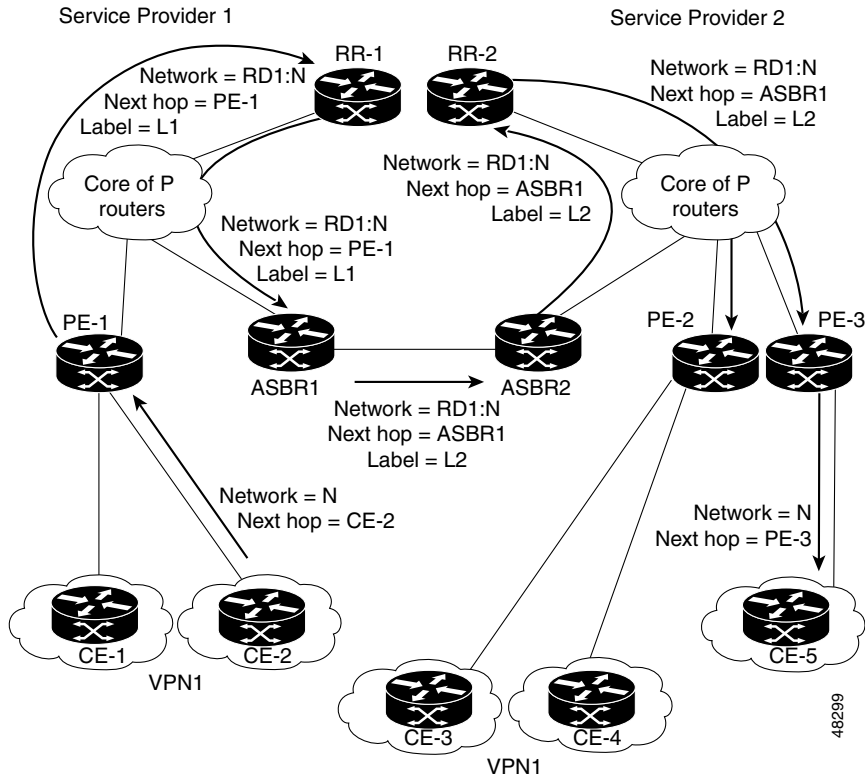
Figure 13-3 Host Routes Propagated to All PEs Between Two Autonomous Systems

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.

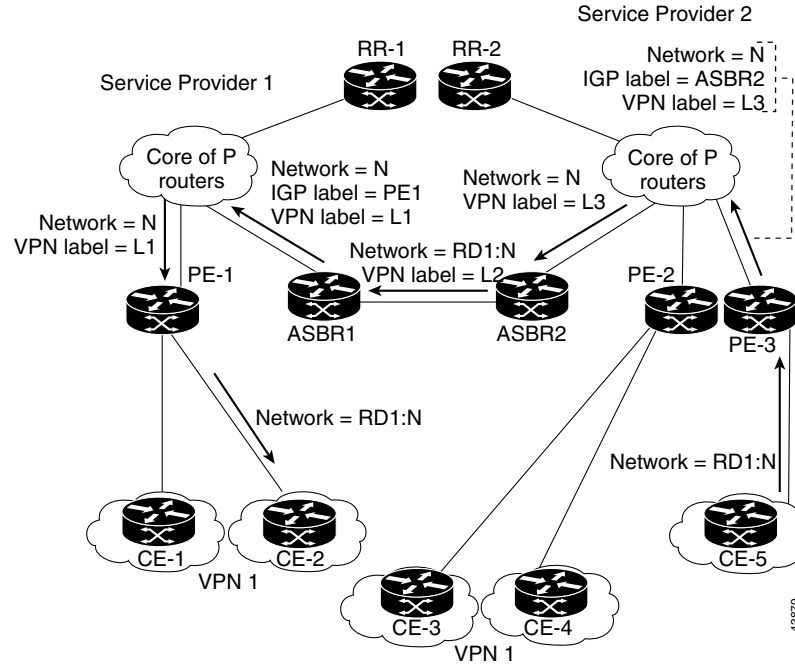
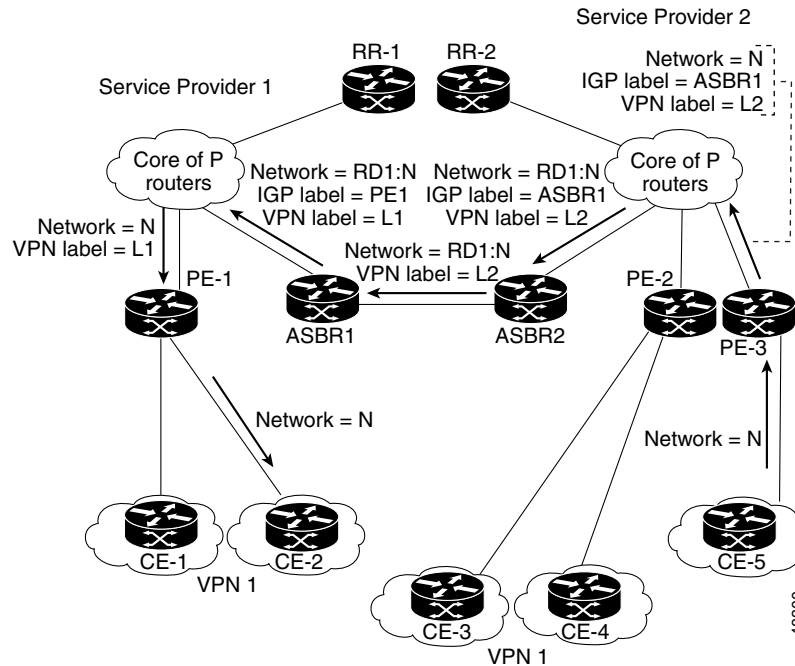
Figure 13-4 Forwarding Packets Between Two Autonomous Systems

Figure 13-5 illustrates shows the same packet forwarding method, except the EBGW 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.

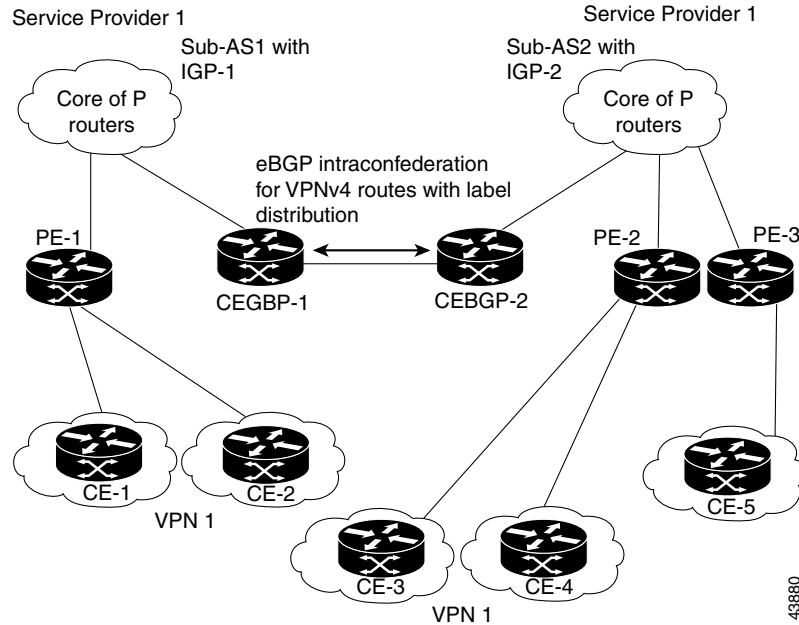
In a confederation, each subautonomous system is fully meshed with other subautonomous systems. The subautonomous systems communicate using an IGP, such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS). Each subautonomous system also has an EBGp connection to the 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 subautonomous systems use EBGP 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.

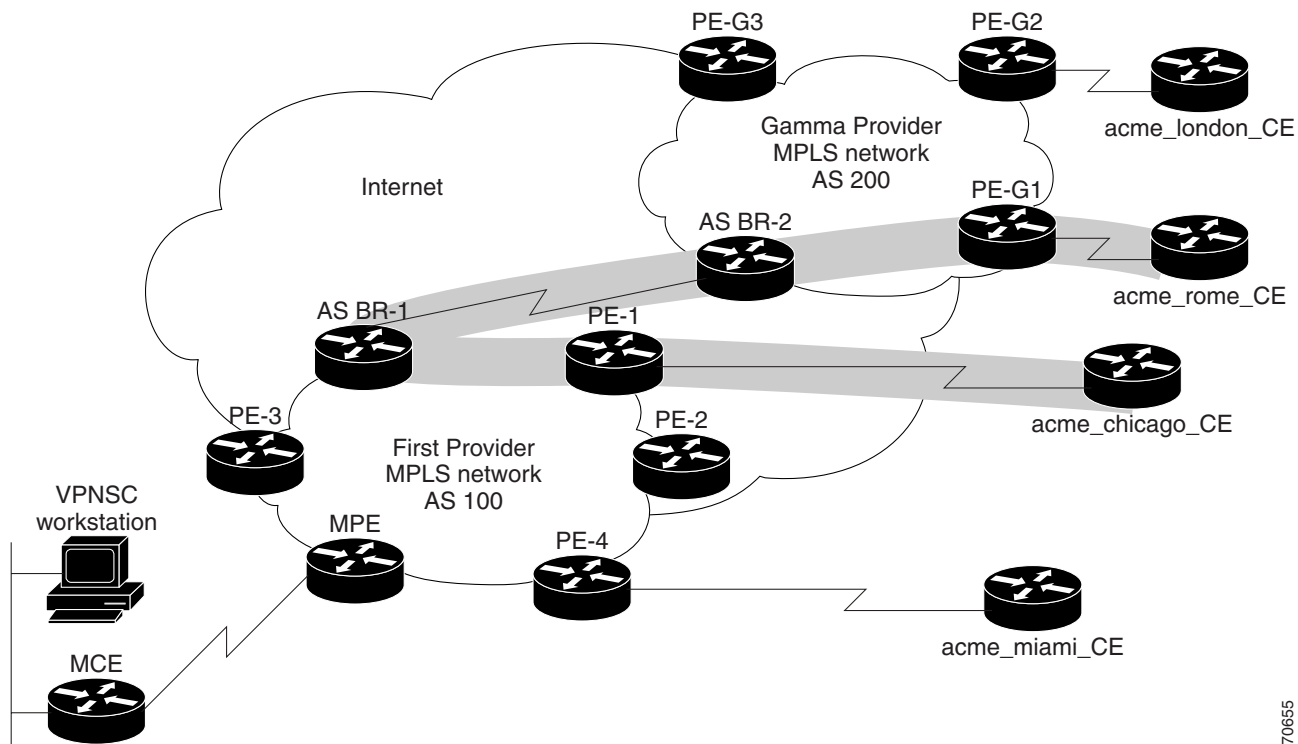
The next-hop-self address is included in the label (as the value of the EBGP next-hop attribute). Within the subautonomous systems, the CEBGP border edge router address is distributed throughout the IBGP neighbors and the two CEBGP border edge routers are known to both confederations.

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

70655

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.

Using Templates to Support Inter-Autonomous System Solutions

This section covers how ISC supports inter-autonomous system (inter-AS) and inter-provider VPNs through ISC templates.

**Note**

ISC currently supports only the inter-AS 10B Hybrid model for L2TPV3 networks. This is the solution documented in this section.

Inter-AS 10B Hybrid Model

The current release of ISC provides two pairs of template scripts for provisioning and decommissioning inter-AS 10B Hybrid VPNs:

- Provisioning and decommissioning VPN-independent inter-AS 10B Hybrid CLIs on an Autonomous System Border Router (ASBR)
- Provisioning and decommissioning VPN-specific inter-AS 10B Hybrid CLIs on an ASBR

Using the second pair of template scripts, the provider can create a new pair of data-files for provisioning and decommissioning a new inter-AS VPN on the ASBR, as and when added. The default inter-AS scripts can be modified to create or change scripts for modifying inter-AS configuration.

The following commands are supported in the VPN-independent inter-AS 10B Hybrid default templates:

- Provisioning resolve in VRF (RiV) VRF for L2TPV3 tunnel on an ASBR
- L2TPV3 tunnel configuration
- ASBR-facing interface provisioning
- BGP configuration:
 - BGP configuration with a **peer-group**
 - eBGP configuration
 - BGP **address-family ipv4** configuration
 - BGP **address-family ipv4 tunnel** configuration
 - BGP **address-family vpnv4** configuration
- Default route configuration through an L2TPV3 tunnel interface

The following commands are supported in the VPN-specific inter-AS 10B Hybrid default templates:

- Provisioning VRF for a customer VPN
- Recommended/standard route target (RT) support for full-mesh and hub-and-spoke VPN types. Spoke RTs are optional.
- RT-rewrite configuration:
 - Extended community (**extcommunity-list**) provisioning
 - Route maps provisioning

Inter-AS RT-Rewrite

ISC supports inter-AS RT-rewrite configuration on the ASBR. Velocity Template Language (VTL) template scripts for provisioning and decommissioning of RT-rewrite commands are provided as part of the inter-AS 10B hybrid templates, covered in the next section. You can edit these VTL scripts to create your own templates for the respective use-case.

Creating the Inter-AS Templates



Note

For additional coverage of creating and using templates in ISC, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). Also see [Appendix B, “Working with Templates and Data Files.”](#)

The default inter-AS templates are provided in the Examples templates directory in ISC. The templates are created from the Service Design window, which you access by choosing:

Service Design > Templates > Examples

The templates for Inter-AS 10b hybrid are:

- Configure_PE_as_ASBR_non_VPN_Specific_Template_TMPL_
- Remove_PE_as_ASBR_non_VPN_Specific_Template_TMPL_
- Configure_PE_as_ASBR_VPN_Specific_Template_TMPL_
- Remove_PE_as_ASBR_VPN_Specific_Template_TMPL_

You can create and change templates, using the default provisioning and decommissioning scripts, based on the respective use-case. Because the inter-AS configurations are mostly a one time setup, the templates are downloaded from the device console only, but are not attached to a service request.

The ISC templates feature supports a basic deployment check to determine whether the template data file was successfully deployed or whether there was any command that failed to deploy. In addition, you can select the data-type for the variables, which facilitates entering the right values during data-file creation in the user interface.

After you successfully create the template data file that contains the inter-AS CLIs, you can download the template data file onto the ASBR or route reflector using the ISC Device Console window, which you access by choosing:

Service Inventory > Device Console

The templates you created under Service Design can be selected for deployment on a device or a device-group.



Note

The ISC templates feature is not model-based, so no template deployment history or stack is saved, no template roll-back is supported, and no template CLI audit is supported when you download the templates using the Device Console. You can also select templates in a service request, and have them downloaded onto the PE routers, in case you need to download specific IBGP commands on the PE routers.



CHAPTER 14

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](#)
- [Running Reports, page 14-2](#)
- [MPLS PE Service Report, page 14-3](#)
- [MPLS Service Request Report, page 14-4](#)
- [MPLS Service Request Report - 6VPE, page 14-5](#)
- [6VPE Supported Devices Report, page 14-6](#)
- [Creating Custom Reports, page 14-7](#)

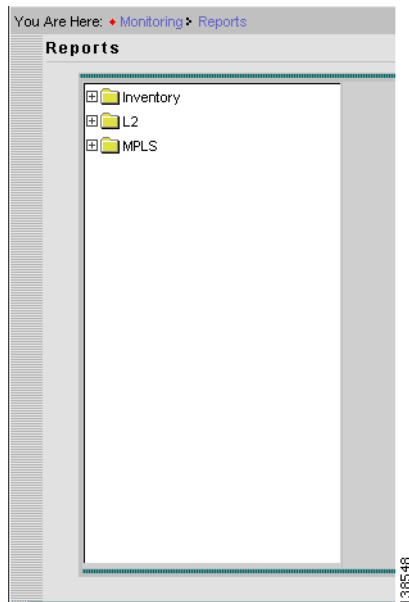
Overview

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 the “Monitoring” chapter in the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). The rest of this chapter provides information about the MPLS reports available in ISC.

Accessing MPLS Reports

To access MPLS reports, perform the following steps.

-
- Step 1** Log in to ISC.
 - Step 2** Go to: **Monitoring > Reports**.
 - Step 3** Click on the MPLS folder to display the available MPLS reports.
- The Reports window appears, as shown in [Figure 14-1](#).

Figure 14-1 Reports List

- Step 4** 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, page 14-7](#), for information on custom reports.

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.

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 PE Service Report

The MPLS PE 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:	*
Output Fields	
PE Role PE Name Policy Type SR State SR ID SR Job ID	
Sorting	
Field:	PE Role Ascending

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 D, “Service Request Transition States”](#)).



Note The **SR State** output does not list service requests in the **CLOSED** state. Service requests in other states are listed, as determined by the filter values.

- **SR ID**—List by service request ID.
- **SR Job ID**—List by service request job ID.

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 14-3](#).

Figure 14-3 MPLS Service Request Report

Layout	
Title:	MPLS SR Report (PE,CE,VPN,SR ID,SR STATE)
Chart Type:	Tabular
Filters (All field values are required, * or a valid value.)	
PE_ROUTER:	* Select
CE_ROUTER:	* Select
Job_ID:	*
SR_STATE:	*
VPN_ID:	* Select
Output Fields	
PE_ROUTER CE_ROUTER Job_ID SR_STATE VPN_ID CREATION_DATE_TIME	
Sorting	
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 D, “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.
- **SR STATE**—Service request states (see [Appendix D, “Service Request Transition States”](#)).



Note The **SR State** output does not list service requests in the **CLOSED** state. Service requests in other states are listed, as determined by the filter values.

- **VPN ID**—List by VPN ID.
- **CREATION DATE TIME**—List by date and time report created.

MPLS Service Request Report - 6VPE

The MPLS Service Request - 6VPE report feature allows you to list service requests as related to PE, CE, VPN, SR ID, SR STATE.

Click the MPLS Service Request Report - 6VPE icon to bring up the window for this report, as shown in [Figure 14-3](#).

Figure 14-4 MPLS Service Request Report - 6VPE

Layout	
Title:	MPLS SR Report - 6VPE (PE,CE,VPN,SR ID,SR STATE)
Chart Type:	Tabular

Filters (All field values are required, * or a valid value.)	
Job_ID:	*
SR_STATE:	*
VPN_ID:	* Select
PE_ROUTER:	* Select
CE_ROUTER:	* Select

Sorting
N/A

Output Fields
 Job_ID
 SR_STATE
 VPN_ID
 PE_ROUTER
 CE_ROUTER
 CREATION_DATE_TIME

Filter Values

- **Job ID**—Service request job IDs.
- **SR STATE**—Service request states (see [Appendix D, “Service Request Transition States”](#)).
- **VPN ID**—Choose some or all (*) VPNs by ID.
- **PE ROUTER**—Choose some or all (*) PE routers.
- **CE ROUTER**—Choose some or all (*) CE routers.

Output Filters

- **Job ID**—List by Job ID.
- **SR STATE**—Service request states (see [Appendix D, “Service Request Transition States”](#)).



Note The **SR State** output does not list service requests in the **CLOSED** state. Service requests in other states are listed, as determined by the filter values.

- **VPN ID**—List by VPN ID.
- **PE ROUTER**—Show PE routers.
- **CE ROUTER**—Show CE routers.
- **CREATION DATE TIME**—List by date and time report created.

6VPE Supported Devices Report



Note

In the ISC GUI, this report is located under **Monitoring > Reports > Inventory**.

Click the 6VPE Supported Devices Report icon to bring up the window for this report, as shown in [Figure 14-3](#).

Figure 14-5 6VPE Supported Devices Report

Layout

Title:6VPE Supported Devices Report

Chart Type:Tabular

Filters (All field values are required, * or a valid value.)

Host Name:*

Management Address:*

Software Version:*

Sorting

Field:Host NameAscending

Output Fields

Host Name
Management Address
Software Version

211636

Filter Values

- **Host Name** – Host name.
- **Management Address** – Management address.
- **Software Version** – Software version.

Output Filters

- **Host Name** – Host name.
- **Management Address** – Management address.
- **Software Version** – Software version.

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 the [Cisco IP Solution Center Infrastructure Reference, 5.1](#) for details on how to modify report configuration files to create custom reports.



APPENDIX A

Sample Configlets

This appendix provides sample configlets for MPLS VPN provisioning in ISC. It contains the following sections:

- [Overview, page A-1](#)
- [L2 Access into L3 MPLS VPN, page A-3](#)
- [CE-PE L3 MPLS VPN \(BGP with full-mesh\), page A-5](#)
- [CE-PE L3 MPLS VPN \(BGP with SOO\), page A-6](#)
- [CE-PE L3 MPLS VPN, page A-7](#)
- [N-PE L3 MPLS VPN \(IPv4, IOS XR, OSPF\), page A-8](#)
- [N-PE L3 MPLS VPN \(IPv6, IOS XR, EIGRP\), page A-12](#)
- [CE-PE L3 MPLS VPN \(Q-in-Q/Second VLAN ID\), page A-16](#)

Overview

The configlets provided in this appendix show the CLIs generated by ISC for particular services and features. Each configlet example provides the following information:

- Service.
- Feature.
- Devices configuration (network role, hardware platform, relationship of the devices and other relevant information).
- Sample configlets for each device in the configuration.
- Comments.



Note

The configlets generated by ISC are only the delta between what needs to be provisioned and what currently exists on the device. This means that if a relevant CLI is already on the device, it does not show up in the associated configlet.



Note

All examples in this appendix assume an MPLS core.

For information on how to view configlets, see [Viewing Configlets Generated by a Service Request, page 6-31](#).

L2 Access into L3 MPLS VPN

Configuration

- Service: L2VPN/Metro Ethernet.
- Feature: Access into L3 MPLS VPN.
- Device configuration:
 - The CE is a Cisco 3550 with IOS 12.1(22)EA1.
Interface(s): F0/13 <-> F0/4.
 - The U-PE is a Cisco 3550 with IOS 12.1(22)EA1.
Interface(s): F0/14.
 - The N-PE is a Cisco 7609 with IOS 12.2(18)SXF.
Interface(s): F2/8.
 - VLAN = 3101.

Configlets

CE	U-PE	N-PE
<pre>! vlan 3101 exit ! interface FastEthernet0/13 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,3101 ! interface Vlan3101 description By VPNSC: Job Id# = 13 ip address 10.19.19.10 255.255.255.252 no shutdown</pre>	<pre>! vlan 3101 exit ! interface FastEthernet0/14 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,3101 ! interface FastEthernet0/4 no keepalive no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 3101 switchport nonegotiate cdp enable no shutdown mac access-group ISC-FastEthernet0/4 in ! mac access-list extended ISC-FastEthernet0/4 deny any host 0100.0ccc.cccc deny any host 0100.0ccc.cccd deny any host 0100.0ccd.cdd0 deny any host 0180.c200.0000 permit any any</pre>	<pre>! ip vrf V5:VPN_sample rd 100:1502 route-target import 100:1602 route-target import 100:1603 route-target export 100:1602 maximum routes 100 80 ! interface FastEthernet2/8 no shutdown ! interface FastEthernet2/8.3101 description FastEthernet2/8.3101 dot1q vlan id=3101. By VPNSC: Job Id# = 13 encapsulation dot1Q 3101 ip vrf forwarding V5:VPN_sample ip address 10.19.19.9 255.255.255.252 no shutdown ! router bgp 100 address-family ipv4 vrf V5:VPN_sample redistribute connected redistribute static exit-address-family</pre>

Comments

- IP Numbered scenario with Dot1q encapsulation for VPN Link.
- The VRF is created on the N-PE device (-s designates that the VRF is joining the VPN as a spoke in a hub-n-spoke topology).
- On the N-PE, the VRF is added to iBGP routing instance with user configured redistribution of connected and static options.
- The VRF is created on the NPE with forwarding associated with the U-PE facing interface.

CE-PE L3 MPLS VPN (BGP with full-mesh)

Configuration

- Service: L3 MPLS VPN.
- Feature: CE-PE BGP with full-mesh.
- Device configuration:
 - The PE is a Cisco 7609 with IOS 12.2(18)SXF.
Interface(s): F2/5.
 - The CE is a Cisco 3550 with IOS 12.2(22)EA1.
Interface(s): F0/13.
 - Routing protocol = BGP.

Configlets

CE	PE
<pre>! vlan 62 exit ! interface FastEthernet0/13 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 62 ! interface Vlan62 description By VPNSC: Job Id# = 29 ip address 10.19.19.42 255.255.255.252 no shutdown ! router bgp 10 neighbor 10.19.19.41 remote-as 100</pre>	<pre>! ip vrf V9:mpls_vpn1 rd 100:1506 route-target import 99:3204 route-target export 99:3204 maximum routes 100 80 ! interface FastEthernet2/5.62 description FastEthernet2/5.62 dot1q vlan id=62. By VPNSC: Job Id# = 29 encapsulation dot1Q 62 ip vrf forwarding V9:mpls_vpn1 ip address 10.19.19.41 255.255.255.252 no shutdown ! router bgp 100 address-family ipv4 vrf V9:mpls_vpn1 neighbor 10.19.19.42 remote-as 10 neighbor 10.19.19.42 activate neighbor 10.19.19.42 allowas-in 2 redistribute connected redistribute static exit-address-family</pre>

Comments

- A full-mesh configuration is created by means of the CERC selected for the VPN policy. As a result, route-target import and route-target export are identical.
- BGP is the routing protocol on the CE-PE access link.
- IP Numbered scenario with dot1q encapsulation for the VPN link.
- The VRF is created on the PE device.
- The VRF is created on the PE with forwarding associated with the CE facing interface.

CE-PE L3 MPLS VPN (BGP with S00)

Configuration

- Service: L3 MPLS VPN.
- Feature: CE-PE.
- Device configuration:
 - The PE is a Cisco 7609 with IOS 12.2(18)SXF.
 - Interface(s): FE2/3.
 - The CE created in ISC.
 - Interface(s): FE1/0/14.
 - Routing protocol = BGP.
 - VPN = hub.

Configlets

CE	PE
<pre>! vlan 3100 exit ! interface FastEthernet1/0/14 no ip address switchport switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,3100 no shutdown ! interface Vlan3100 description By VPNSC: Job Id# = 12 ip address 10.19.19.6 255.255.255.252 no shutdown ! router ospf 3500 network 10.19.19.4 0.0.0.3 area 12345</pre>	<pre>! ip vrf V4:VPN_sample-s rd 100:1501 route-target import 100:1602 route-target export 100:1603 maximum routes 100 80 ! interface FastEthernet2/3.3100 description FastEthernet2/3.3100 dot1q vlan id=3100. By VPNSC: Job Id# = 12 encapsulation dot1Q 3100 ip vrf forwarding V4:VPN_sample-s ip address 10.19.19.5 255.255.255.252 no shutdown ! router ospf 2500 vrf V4:VPN_sample-s redistribute bgp 100 subnets network 10.19.19.4 0.0.0.3 area 12345 ! router bgp 100 address-family ipv4 vrf V4:VPN_sample-s redistribute connected redistribute ospf 2500 vrf V4:VPN_sample-s match internal external 1 external 2 redistribute static exit-address-family</pre>

Comments

- IP Numbered scenario with dot1q encapsulation for the VPN link.
- The VRF is created on PE device (VPN is joining as a spoke).
- On PE, the VRF is added to iBGP routing instance with user configured redistribution of connected and static options.
- The VRF is created on the PE with forwarding associated with the CE-facing interface.

CE-PE L3 MPLS VPN

Configuration

- Service: L3 MPLS VPN.
- Feature: CE-PE.
- Device configuration:
 - The PE is a Cisco 7603 with IOS 12.2(18)SXD7.
Interface(s): FE2/25.
 - The CE is an Cisco 3750ME-I5-M with IOS 12.2(25)EY2.
Interface(s): FE1/0/6.
 - VPN = spoke.

Configlets

CE	PE
<pre>! vlan 890 exit ! interface FastEthernet1/0/6 no ip address switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 890 no shutdown ! interface Vlan890 description By VPNSC: Job Id# = 336 : SR Id# = 336 ip address 10.10.75.2 255.255.255.252 no shutdown ! router bgp 120 neighbor 10.10.75.1 remote-as 100 no auto-summary</pre>	<pre>! ip vrf V60:TestVPN-s rd 100:8069 route-target import 100:1891 route-target export 100:1892 ! interface FastEthernet2/25.890 description FastEthernet2/25.890 dot1q vlan id=890. By VPNSC: Job Id# = 336 : SR Id# = 336 encapsulation dot1Q 890 ip vrf forwarding V60:TestVPN-s ip address 10.10.75.1 255.255.255.252 no shutdown ! router bgp 100 no auto-summary address-family ipv4 vrf V60:TestVPN-s neighbor 10.10.75.2 remote-as 120 neighbor 10.10.75.2 activate neighbor 10.10.75.2 route-map SetSOO_V60:TestVPN-s_100:100 in exit-address-family ! route-map SetSOO_V60:TestVPN-s_100:100 permit 10 set extcommunity soo 100:100</pre>

Comments

- IP Numbered scenario with dot1q encapsulation for the VPN link.
- The VRF is created on the PE device.
- `neighbor 10.10.75.2 remote-as 120` is created as a result of the policy having the CE BGP AS ID set to 120.
- The VRF is created on the PE with forwarding associated with the CE-facing interface.
- On the PE, BGP defines a route-map for the CE neighbor.
- The associated route map sets the extended community attribute to SOO, which is the community value (SOO pool value defined in ISC).

N-PE L3 MPLS VPN (IPv4, IOS XR, OSPF)

Configuration

- Service: L3 MPLS VPN.
- Feature: IPv4 with IOS XR.
- Device configuration:
 - The N-PE is a Cisco 12000 router with IOS XR.
 - Routing protocol = OSPF.

Configlets

N-PE

(See the extended code example below.)

```
<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <Delete>
    <Configuration Source="CurrentConfig">
      <InterfaceConfigurationTable>
        <InterfaceConfiguration>
          <Naming>
            <Name>GigabitEthernet0/1/1/1.856</Name>
            <Active>act</Active>
          </Naming>
          <Shutdown>true</Shutdown>
        </InterfaceConfiguration>
      </InterfaceConfigurationTable>
    </Configuration>
  </Delete>
  <Set>
    <Configuration Source="CurrentConfig">
      <VRFTable>
        <VRF>
          <Naming>
            <Name>ICICI_VPN_1</Name>
          </Naming>
          <AFI_SAFITable>
            <AFI_SAFI>
              <Naming>
                <AFI>IPv4</AFI>
                <SAFI>Unicast</SAFI>
              </Naming>
            </AFI_SAFI>
          </AFI_SAFITable>
          <BGP>
            <ImportRouteTargets>
              <RouteTargetTable>
                <RouteTarget>
                  <Naming>
                    <Type>AS</Type>
                    <AS>100</AS>
                    <ASIndex>1</ASIndex>
                  </Naming>
                </RouteTarget>
              </RouteTargetTable>
            </ImportRouteTargets>
          </BGP>
        </VRF>
      </VRFTable>
    </Configuration>
  </Set>
</Request>
```

```

        <ExportRouteTargets>
          <RouteTargetTable>
            <RouteTarget>
              <Naming>
                <Type>AS</Type>
                <AS>100</AS>
                <ASIndex>1</ASIndex>
              </Naming>
              <True>true</True>
            </RouteTarget>
          </RouteTargetTable>
        </ExportRouteTargets>
      </BGP>
    </AFI_SAFI>
  </AFI_SAFITable>
</VRF>
</VRFTable>
<InterfaceConfigurationTable>
  <InterfaceConfiguration>
    <Naming>
      <Name>GigabitEthernet0/1/1/1.856</Name>
      <Active>act</Active>
    </Naming>
    <Description>GigabitEthernet0/1/1/1.856 dot1q vlan id=856. By VPNSC: Job Id# =
116</Description>
    <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
    <VLANSubConfiguration>
      <VLANIdentifier>
        <VlanType>VLANTypeDot1q</VlanType>
        <FirstTag>856</FirstTag>
      </VLANIdentifier>
    </VLANSubConfiguration>
    <VRF>ICICI_VPN_1</VRF>
    <IPv4Network>
      <Addresses>
        <Primary>
          <IPAddress>10.10.56.1</IPAddress>
          <Mask>255.255.255.252</Mask>
        </Primary>
      </Addresses>
    </IPv4Network>
  </InterfaceConfiguration>
</InterfaceConfigurationTable>
<BGP>
  <AS>
    <Naming>
      <AS>0</AS>
    </Naming>
    <FourByteAS>
      <Naming>
        <AS>100</AS>
      </Naming>
    </FourByteAS>
    <VRFTable>
      <VRF>
        <Naming>
          <Name>ICICI_VPN_1</Name>
        </Naming>
        <VRFGlobal>
          <Exists>true</Exists>
          <RouteDistinguisher>
            <Type>AS</Type>
            <AS>100</AS>
            <ASIndex>8064</ASIndex>
          </RouteDistinguisher>

```

```

    <VRFGlobalAFTable>
      <VRFGlobalAF>
        <Naming>
          <AF>IPv4Unicast</AF>
        </Naming>
        <Enabled>true</Enabled>
        <Redistribution>
          <ConnectedRoutes/>
          <OSPFRouteTable>
            <OSPFRoutes>
              <Naming>
                <OSPFInstanceName>100</OSPFInstanceName>
              </Naming>
              <RedistType>21</RedistType>
              <DefaultMetric>20000</DefaultMetric>
            </OSPFRoutes>
          </OSPFRouteTable>
          <StaticRoutes/>
        </Redistribution>
      </VRFGlobalAF>
    </VRFGlobalAFTable>
  </VRFGlobal>
</VRF>
</VRFTable>
</FourByteAS>
</AS>
</BGP>
<OSPF>
  <ProcessTable>
    <Process>
      <Naming>
        <InstanceName>100</InstanceName>
      </Naming>
      <Start>true</Start>
      <VRFTable>
        <VRF>
          <Naming>
            <VRFName>ICICI_VPN_1</VRFName>
          </Naming>
          <VRFStart>true</VRFStart>
          <Redistribution>
            <RedistributeTable>
              <Redistribute>
                <Naming>
                  <ProtocolType>rip</ProtocolType>
                  <InstanceName>rip</InstanceName>
                </Naming>
                <Classful>>false</Classful>
              </Redistribute>
              <Redistribute>
                <Naming>
                  <ProtocolType>static</ProtocolType>
                  <InstanceName>static</InstanceName>
                </Naming>
                <Classful>>false</Classful>
              </Redistribute>
            </RedistributeTable>
          </Redistribution>
        </VRF>
      </VRFTable>
    </Process>
  </ProcessTable>
  <AreaTable>
    <Area>
      <Naming>
        <IntegerID>100</IntegerID>
      </Naming>
      <NameScopeTable>

```

```

        <NameScope>
          <Naming>
            <Interface>GigabitEthernet0/1/1/1.856</Interface>
          </Naming>
          <Running>true</Running>
        </NameScope>
      </NameScopeTable>
      <Running>true</Running>
    </Area>
  </AreaTable>
  <DefaultInformation>
    <AlwaysAdvertise>true</AlwaysAdvertise>
  </DefaultInformation>
</VRF>
</VRFTTable>
</Process>
</ProcessTable>
</OSPF>
</Configuration>
</Set>
<Commit/>
</Request>

```

Comments

- In IOS XR, device configuration is specified in XML format.
- With respect to the XML schemas, different versions of IOS XR will generate different XML configlets. However the configurations will be almost identical, except for changes in the XML schema.
- There are different cases to consider. For example, when a service request is decommissioned or modified, the XML configuration will slightly differ.

N-PE L3 MPLS VPN (IPv6, IOS XR, EIGRP)

Configuration

- Service: L3 MPLS VPN.
- Feature: N-PE running IOS XR 3.5.x.
- Device configuration:
 - The N-PE is a Cisco 12000 router with IOS XR 3.5.x.
 - Routing protocol = EIGRP.

Configlets

N-PE

(See the extended code example below.)

```
<?xml version="1.0" encoding="UTF-8"?>
<Request MajorVersion="1" MinorVersion="0">
  <CLI>
    <Configuration>
      interface GigabitEthernet0/1/1/1.840

      ipv6 address fec0:140:9834::/64

      exit

    </Configuration>
  </CLI>
  <Delete>
    <Configuration Source="CurrentConfig">
      <EIGRP>
        <ProcessTable>
          <Process>
            <Naming>
              <ASNumber>100</ASNumber>
            </Naming>
            <VRFTTable>
              <VRF>
                <Naming>
                  <VRFName>V10:ICICI_VPN</VRFName>
                </Naming>
                <VRF_AFTTable>
                  <VRF_AF>
                    <Naming>
                      <VRF_AFTType>IPv4</VRF_AFTType>
                    </Naming>
                    <AutoSummary/>
                  </VRF_AF>
                </VRF_AFTTable>
              </VRF>
            </VRFTTable>
          </Process>
        </ProcessTable>
      </EIGRP>
      <InterfaceConfigurationTable>
        <InterfaceConfiguration>
          <Naming>
```

```

        <Name>GigabitEthernet0/1/1/1.840</Name>
        <Active>act</Active>
    </Naming>
    <Shutdown>true</Shutdown>
</InterfaceConfiguration>
</InterfaceConfigurationTable>
</Configuration>
</Delete>
<Set>
    <Configuration Source="CurrentConfig">
        <InterfaceConfigurationTable>
            <InterfaceConfiguration>
                <Naming>
                    <Name>GigabitEthernet0/1/1/1.840</Name>
                    <Active>act</Active>
                </Naming>
                <Description>GigabitEthernet0/1/1/1.840 dot1q vlan id=840. By VPNSC: Job Id# =
50</Description>
                <InterfaceModeNonPhysical>Default</InterfaceModeNonPhysical>
                <VLANSubConfiguration>
                    <VLANIdentifier>
                        <VlanType>VLANTypeDot1q</VlanType>
                        <FirstTag>840</FirstTag>
                    </VLANIdentifier>
                </VLANSubConfiguration>
                <VRF>V10:ICICI_VPN</VRF>
            </InterfaceConfiguration>
        </InterfaceConfigurationTable>
        <BGP>
            <AS>
                <Naming>
                    <AS>0</AS>
                </Naming>
                <FourByteAS>
                    <Naming>
                        <AS>100</AS>
                    </Naming>
                <VRFTable>
                    <VRF>
                        <Naming>
                            <Name>V10:ICICI_VPN</Name>
                        </Naming>
                        <VRFGlobal>
                            <Exists>true</Exists>
                            <VRFGlobalAFTable>
                                <VRFGlobalAF>
                                    <Naming>
                                        <AF>IPv6Unicast</AF>
                                    </Naming>
                                    <Enabled>true</Enabled>
                                    <Redistribution>
                                        <EIGRPRouteTable>
                                            <EIGRPRoutes>
                                                <Naming>
                                                    <EIGRPInstanceName>120</EIGRPInstanceName>
                                                </Naming>
                                            </EIGRPRoutes>
                                        </EIGRPRouteTable>
                                    </Redistribution>
                                </VRFGlobalAF>
                            </VRFGlobalAFTable>
                        </VRFGlobal>
                    </VRF>
                </VRFTable>
            </AS>
        </BGP>
    </Configuration>
</Set>

```

```

        </FourByteAS>
    </AS>
</BGP>
<EIGRP>
    <ProcessTable>
        <Process>
            <Naming>
                <ASNumber>100</ASNumber>
            </Naming>
            <VRFTTable>
                <VRF>
                    <Naming>
                        <VRFName>V10:ICICI_VPN</VRFName>
                    </Naming>
                    <Enabled>true</Enabled>
                    <VRF_AFTable>
                        <VRF_AF>
                            <Naming>
                                <VRF_AFType>IPv4</VRF_AFType>
                            </Naming>
                            <Enabled>true</Enabled>
                            <RedistributeTable>
                                <Redistribute>
                                    <Naming>
                                        <Protocol>BGP</Protocol>
                                        <SecondASNumber>100</SecondASNumber>
                                    </Naming>
                                    <PolicySpecified>>false</PolicySpecified>
                                </Redistribute>
                            </RedistributeTable>
                        </VRF_AF>
                    </VRF_AFTable>
                    <DefaultMetric>
                        <BW>2000</BW>
                        <Delay>2001</Delay>
                        <Reliability>200</Reliability>
                        <Load>201</Load>
                        <MTU>20000</MTU>
                    </DefaultMetric>
                    <InterfaceTable>
                        <Interface>
                            <Naming>
                                <InterfaceName>GigabitEthernet0/1/1/1.840</InterfaceName>
                            </Naming>
                            <Enabled>true</Enabled>
                        </Interface>
                    </InterfaceTable>
                    <AutonomousSystem>120</AutonomousSystem>
                </VRF>
            </VRFTTable>
        </Process>
    </ProcessTable>
</EIGRP>
</Configuration>
</Set>
<Commit/>
</Request>Comments

```

- In IOS XR, device configuration is specified in XML format.
- With respect to the XML schemas, different versions of IOS XR will generate different XML configlets. However the configurations will be almost identical, except for changes in the XML schema.

- There are different cases to consider. For example, when a service request is decommissioned or modified, the XML configuration will slightly differ.

CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID)

Configuration

- Service: L3 MPLS VPN.
- Feature: CE-PE. Q-in-Q (second VLAN ID) is configured on the PE.
- Device configuration:
 - The N-PE is a Cisco 7606-S with IOS 12.2(33)SRC, and with an ES20 line card.
Interface(s): GE2/0/15.
 - The CE is a Cisco 2811.
Interface(s): FE0/0.
 - VPN = spoke.

Configlets

CE	N-PE
<pre>! interface FastEthernet0/0.158 description FastEthernet0/0.158 dot1q vlan id=158. By VPNSC: Job Id# = 239 encapsulation dot1Q 158 ip address 10.1.1.98 255.255.255.252 no shutdown ! ip route 0.0.0.0 0.0.0.0 FastEthernet0/0.158</pre>	<pre>! ip vrf V15:MPLS-1 rd 100:6812 route-target import 100:7000 route-target import 100:7001 route-target export 100:7000 ! interface GigabitEthernet2/0/15.158 description GigabitEthernet2/0/15.158 dot1q vlan id=158. By VPNSC: Job Id# = 239 encapsulation dot1Q 158 second-dot1q 1502 ip vrf forwarding V15:MPLS-1 ip address 10.1.1.97 255.255.255.252 no shutdown ! router bgp 100 address-family ipv4 vrf V15:MPLS-1 redistribute connected redistribute static exit-address-family</pre>

Comments

- Encapsulation must be dot1q; SVI disabled.
- IOS support only. There is no Q-in-Q support for IOS XR.
- The resulting CLI configuration command is:


```
encapsulation dot1Q <VID-1> second-dot1q <VID-2>
```

 - VID-1 can be assigned by ISC VLAN ID resource pools, or manually.
 - VID-2 must be added manually. There is no support for autopick ID for the second VLAN ID.
- Platforms/IOS versions which support the command include, but are not limited to:
 - Cisco 7600/SRBx with ES-20, SIP400 + 2, and 5-port GE-V2 SPA.
 - Cisco 7600/SRCx ES-20, SIP400 + 2, 5-port GE-V2 SPA, and 10GE-V2 SPA.
 - Cisco 7200 NPE-G1 with IOS 12.4 mainline.

- Cisco 7200 NPE-G2 with IOS 12.4(4)XD.
- There is a new template variable for second VLAN ID: `$Second_PE_Vlan_ID`.
- Network configurations supported include:
 - PE only.
 - PE-CE with managed and unmanaged CEs.



Note SecondVLAN ID is configured on the PE only, not the CE.

For additional coverage of Q-in-Q support in ISC, see the coverage of the Second VLAN ID attribute in the section [Creating an MPLS VPN PE-CE Service Request, page 6-7](#).



APPENDIX **B**

Working with Templates and Data Files

This appendix describes how to use templates and data files with ISC policies and service requests. It contains the following sections:

- [Overview, page B-1](#)
- [Using Templates with ISC Policies, page B-4](#)
- [Using Templates with Service Requests, page B-8](#)



Note

For an overview of the Template Manager and how templates and data files are created in ISC, see Chapter 6, “Service Design” and Appendix D, “Template Usage” in the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

Overview

ISC’s Template Manager allows you to create, manage, and store templates and associated data files. The purpose of using templates is to provide a means to download free-form CLIs to a device, in order to deploy commands and configurations not normally supported by ISC. Templates are written in the Velocity Template Language and are generally comprised of IOS (and IOS XR) device CLI configurations. Optionally, you can set variables (also defined in Velocity) that are substituted with data stored in data files. The template and data file information is downloaded to the device at the time of service activation. The information in this appendix assumes the templates (including subtemplates, if applicable) and (optional) data files have been set up.



Note

You can also create data files “on demand” during service request creation, as covered in later sections of this appendix.

This overview section covers the following topics:

- [Summary of Template Manager Features, page B-1](#)
- [Template and Data File Workflow, page B-3](#)

Summary of Template Manager Features

This section highlights key features of template and data file support in ISC, especially those that have an impact on working with policies and service requests.

Template Attributes

The ISC template mechanism allows you to differentiate templates by specifying (optional) attributes on a template, including:

- Device type
- Line card type
- Port type
- Software version (IOS or IOS XR)

These attributes are set through a drop-down list when setting up the template in Template Manager. ISC uses these attributes to automatically select the template/data file that most closely matches the device defined within the service request. See the section [Using Templates with Service Requests, page B-8](#), for additional information.

Associating Templates at the Policy Level

ISC supports the association of templates and data files in policies.

Enhanced Subtemplate Support

A new attribute in the Template Editor allows subtemplates to be associated with a template. ISC supports dynamic instantiation of subtemplates based on device attributes. While creating the subtemplates, values for these identifiers must be provided by the operator.

Dynamic Data File Creation

The user can create a data file during service request creation and associate it to the template copied from the associated policy. This functionality extends data file creation from the Template wizard to doing so directly from the service request wizard Template Association screen. In addition, you can modify any or all variables that are part of the template/data file attached to a service request and apply the updated template/data file without removing the entire service.

Automatic Application of Negate Templates

To remove a configuration created from a template/data file, a negate template must be applied to the existing service. This is no longer a manual process in ISC. You create both the positive and negate template. You can assign a positive template/data file to a policy. ISC calls the appropriate negate template at the appropriate time, as the negate template has a direct relationship with the deploy template. ISC determines which negate template to use, based on the service request action requested (for example, deploying or decommissioning a service). The negate template has the same name as the template, with the addition of the suffix .Negate. The negate template does not share the data file of the deploy template. The negate template must have its own data file defined.

Compatibility of the Template Mechanism with Previous ISC Releases

ISC maintains compatibility with the template mechanism in previous ISC releases. Templates created in earlier versions of ISC work “as is,” without any modifications to the templates or the workflow. In the case of a policy in the system that was created in an earlier ISC release, the GUI workflow for associating templates/data files is not visible. In such a case, the operator adds the template and data files during service deployment, as in previous releases of ISC.

Template Support for IOS and IOS XR

The template mechanism is supported for both IOS and IOS XR devices. For IOS XR devices, the configlet generated from templates/data files contains CLI commands and not XML statements. For IOS XR devices, template support is provided as CLI commands. For IOS devices, the operator can download a template configlet using the device console.

RBAC Support for Template Usage

Templates and data files are only accessible to users with the proper RBAC role. A permission type for data files has been added. The permissions allowed for the data files are view, create, modify, and delete. Operators cannot view templates/data files assigned to other roles, and are not permitted to deploy templates/data files to which they do not have access. See the [Cisco IP Solution Center Infrastructure Reference, 5.1](#) for more information on RBAC support for templates/data files.

Template Variables

Template variables support most ISC repository variables for MPLS, L2VPN, VPLS, and FlexUNI/EVC. For a list of supported template variables, see the “Devices” chapter of the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

Importing and Exporting Templates

ISC provides a mechanism to import and export templates and data files. See the [Cisco IP Solution Center Infrastructure Reference, 5.1](#) for more information.

Template and Data File Workflow

This section summarizes the basic operations involved in setting up and using templates, data files, and negate templates in ISC.

Basic Template Manager Functions

- Create templates and negate templates for different configurations.
- Specify device attributes for the templates.
- Associate subtemplates to templates, if applicable
- Create data files for the subtemplates.
- Create a negate template for each subtemplate.
- Create data files for the negate templates.
- Create a super template and attach subtemplates to it.

These basic Template Manager functions are documented in the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). See that guide for more information on these tasks.

Policy-Level Template Functions

- Create a policy and enable template support for the policy.
- Associate templates and (optionally) data files to the policy, if desired.

For information on how to associate templates and data files at the policy level, see the section [Using Templates with ISC Policies, page B-4](#), in this appendix.

Service Request-Level Template Functions



Note

When a policy is only associated with a template and no data file, then during creation of a service request using that policy, automatic selection of a data file for that template takes place, if the template has only one data file. If the template does not have a data file, then one must be created for that template and associated to the service request before saving is permitted.

- Create a service request and associate template(s) to a link.
- Deploy the service request on a device (for example, a 7600).
- The subtemplate and corresponding data file for the 7600 are autoselected for deployment.
- A configlet is generated from the subtemplate.
- Decommission the service request.
- The negate template for the subtemplate is autoselected and deployed.

For information on how to use templates and data files in service requests, see the section [Using Templates and Data Files with Service Requests, page B-12](#), in this appendix.

Using Templates with ISC Policies

This section provides information on how to enable template support and associate templates/data files with ISC policies. It contains the following sections:

- [Overview of Template Support in ISC Policies, page B-4](#)
- [Associating Templates and Data Files to a Policy, page B-4](#)

Overview of Template Support in ISC Policies

ISC supports associating templates/data files to a service policy. This minimizes steps in the provisioning workflow and also reduces potential errors that can occur if an incorrect template/data file is selected during service creation. In the Policy Editor workflow, after the policy attributes are set, a new Templates Association window appears. The Enable Templates check box that appears in this window allows you to enable template association for the policy and to specify templates/data files to be available for service requests based on the policy. More than one template/data file can be associated to the policy. Each template/data file can be associated to a device role. The available device roles are determined by the policy type. Later, at the time of service request creation, templates are only available if the device type matches the type specified for the template within the policy.

**Note**

In the case of older policies that were created before ISC 5.1, the previous method of supporting templates in policies is maintained for backward compatibility.

Associating Templates and Data Files to a Policy

This section describes how to associate templates and data files to an ISC policy. These features also apply in the case of editing a policy.

After the policy attributes are set for a policy, the Template Association window appears in the workflow, as shown in [Figure B-1](#).

Figure B-1 *Template Association Window*

Attribute	Value
Template Enable:	☐

- Step 5 of 5 -

< Back Next > Finish Cancel

211678

This window is where you associate the templates/data files as a final step before clicking the Finish button and saving the policy settings.

Perform the following steps to associate template(s)/data file(s) with the policy.

- Step 1** Check the **Template Enable** check box to enable template use in service requests based on this policy. This check box is unchecked by default.

The GUI updates with fields allowing you to associate templates/data files to the policy, as shown in [Figure B-2](#).

Figure B-2 *Template Association Window with Template Enable Checked*

Attribute	Value
Template Enable:	☒
Associate Template/Datafile(s) :	
☐ Role Type	Template/Data File
	Editable

Add Delete

- Step 5 of 5 -

< Back Next > Finish Cancel

211679

Step 2 Click the **Add** button to add a row in which to specify associated templates/data files.

A new row appears in the GUI, providing fields to set the role type, specify templates/data files, and specify if the template/data file is editable within service requests based on the policy.

Step 3 In the Role Type column, choose a device role from the drop-down list.

The role selections might include:

- N-PE
- PE-AGG
- U-PE
- CE (MULTI_VRF)
- CE (MANAGED)
- MVRF



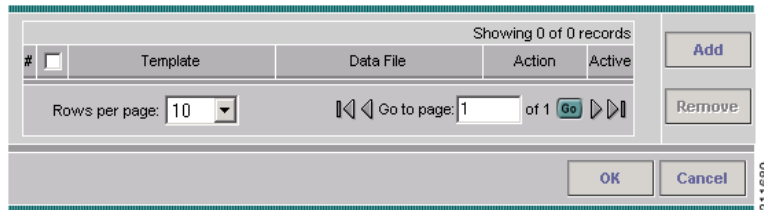
Note

The available device roles in the drop-down list are determined by the policy type.

Step 4 To add a template/data file click the **Add** link in the Template/Data File column.

The Add/Remove Templates window appears, as shown in [Figure B-3](#).

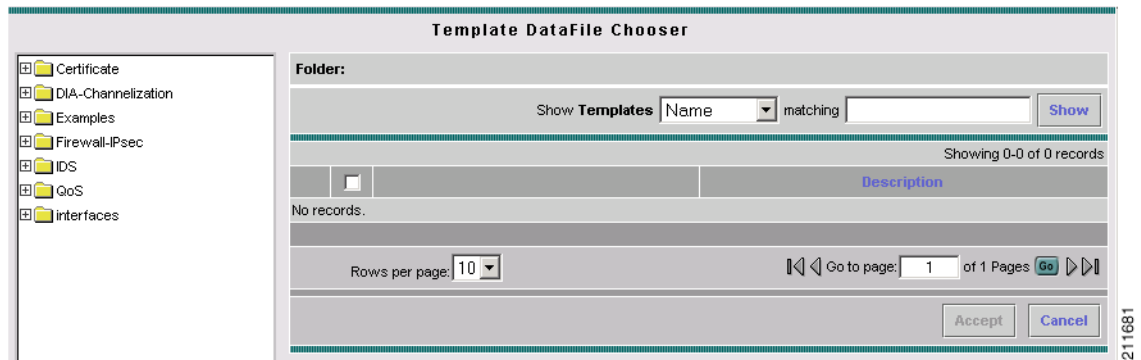
Figure B-3 Add/Remove Template Pop-Up



Step 5 Click the **Add** button to select a template/data file to associate with the policy.

The Template Datafile Chooser window appears, as shown in [Figure B-4](#).

Figure B-4 Template Datafile Chooser Window



This is a standard Template Manager window used to navigate to and choose templates and (optionally) data files in ISC.

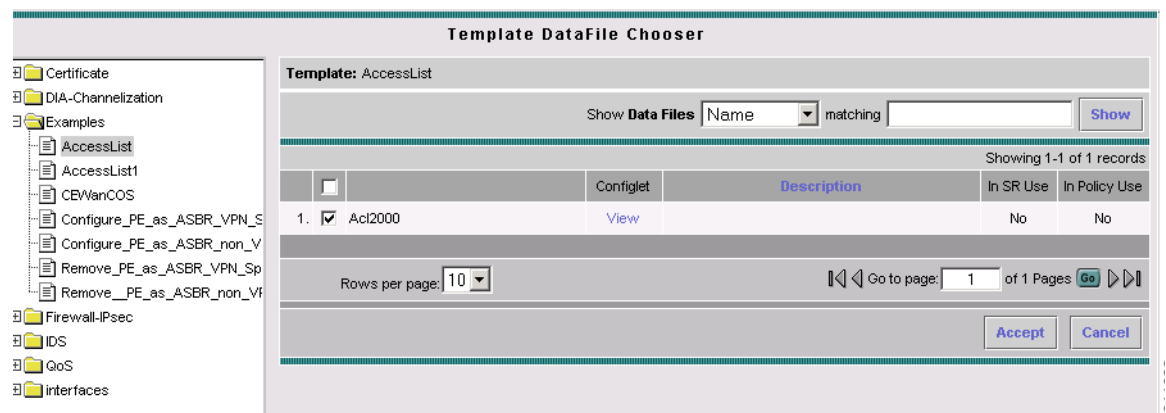
**Note**

The following steps involving the Template Datafile Chooser window assume a familiarity with the functionality of the window. For additional information about Template Manager and how templates and data files are created and managed in ISC, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). The steps shown here are for example purposes. You must modify the steps as required for your environment. For example, you might want to choose only a template file or both a template file and a data file to associate with the policy. Both scenarios are supported.

Step 6 Navigate to a template in the folder tree and click it to select it.

The template is listed in the right side of the GUI, along with any data files that are associated with it, as shown in [Figure B-5](#).

Figure B-5 Template Datafile Chooser Window with Template and Data File Listed



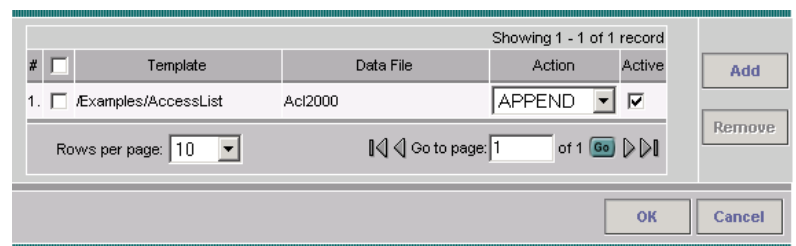
Step 7 Check the check box to the left of a data file name and click the **Accept** button.

**Note**

You can select only the template or both template and data file at this stage, depending on your needs, and whether or not a data file exists for the template.

The Template Datafile Chooser window closes and the selected template/data file appears listed in the Add/Remove Templates window, as shown in [Figure B-6](#).

Figure B-6 Add/Remove Templates Window with Template Listed



If you did not choose a data file, then the Datafile column is blank.

Step 8 Check the check box to the left of the template name to choose the template.

- Step 9** Under Action, use the drop-down list and choose **APPEND** or **PREPEND**.
Append tells ISC to append the template-generated CLIs to the regular ISC (non-template) CLIs (configlet). Prepend is the reverse (adds the template to the beginning of the configlet).
- Step 10** Choose **Active** to use this template for service requests based on this policy.
If you do not choose Active, the template is not used.
- Step 11** To associate additional templates/data files with the policy click **Add** in the Add/Remove Templates window and repeat the appropriate steps to add other templates/data files.
- Step 12** To remove a template row from the window, check a template and click the **Remove** button to remove the template from the list.
- Step 13** When you are satisfied with the selections in the Add/Remove Templates window, click **OK**.
The Template Association window appears with the template(s)/data file(s) listed as active link(s). If you have added more than one template/data file, they appear in a comma-separated list of links.
You can click on any link to return to the Add/Remove Templates window, in order to edit/update the template/data file information.
- Step 14** Check the **Edit** check box to make the template/data file attributes editable in service requests based on the policy.
- Step 15** To add additional templates/data files for a given role to the policy, you can click the **Add** button in the Template Association window and repeat the steps outlined above.
- Step 16** To delete templates/data files that have been associated to the policy, check a template/data file to choose it.
Then click the **Delete** button to delete it from the Template Association window.
- Step 17** When you are finished associating the template(s)/data file(s) to the policy, click the **Finish** button in the Template Association window.
The attributes for the policy are saved and the policy creation or modification is complete.
-

Using Templates with Service Requests

This section provides information on templates and data files with a service request. It contains the following sections:

- [Overview of Template Use in Service Requests, page B-8](#)
- [Using Templates and Data Files with Service Requests, page B-12](#)

Overview of Template Use in Service Requests

This section provides overview information about template usage in service requests. It covers the following topics:

- [Associating Templates to a Service Request, page B-9](#)
- [Associating Subtemplates During Service Provisioning, page B-9](#)
- [Creating Data Files During Service Request Creation, page B-10](#)

- [Using Negate Templates to Decommission Template Configurations, page B-11](#)
- [Using Templates and Data Files with Service Requests, page B-12](#)

For details on how these features are implemented in the ISC GUI, see the section [Using Templates and Data Files with Service Requests, page B-12](#).

Associating Templates to a Service Request

The template mechanism in ISC provides a way to add additional configuration information to a device configuration generated by a service request. To use the template mechanism, the policy on which the service request is based must have been set to enable templates. Optionally, templates and data files to be used by the service request can be specified in the policy. During service request creation, templates/data files can be added to a device configuration if the operator has the appropriate RBAC permission to do so. See the section [Choosing a Template in the Service Request Workflow, page B-12](#) for how to choose templates/data files in the service request workflow.

Associating Subtemplates During Service Provisioning

All templates can be used by other templates as building blocks. The template using other templates is called a super template. The template being used is called a subtemplate. A new attribute in the Template Editor allows subtemplates to be associated with a super template. The super template instantiates all required subtemplates by passing values for the variables in the subtemplate. After instantiation, the super template puts the configlets generated for the subtemplate into the super template. ISC branches templates into subtemplates based on device type, line card type, port type, role type, and software versions. These optional attributes are set while creating the subtemplates. The subtemplates are selected based on the following matching criteria:

- Only exact matches are recognized for the card type and port type attributes. No wild card match is allowed for these attributes.
- Only an exact match is recognized for the device type attribute.
- For the software version attribute, the match is done for a software version equal to the current version, if available. If not, the previous highest version is matched.
- If exact matching attributes are not found, then the match proceeds with the criteria described in [Table B-1](#). An information message listing the exactly matched subtemplates of the super-template is shown if and only if any of the matching criteria are met.
- If none of the attributes are matched, then the default subtemplate is applied.
- If no default subtemplate exists, a subtemplate with all null attribute values is matched.
- If none of the rows specified in the table match, then ISC looks for subtemplates that are marked as device default, or else version default. If no subtemplates are marked as such, then no matching subtemplates are picked. A warning message is displayed.

The matching criteria are summarized in [Table B-1](#).

Table B-1 **Default SubTemplate Matching Criteria**

Matching Order	Role Type	Device Type	Line Card	Port Type	Software Version
1	Exact Match	Exact Match	Exact Match	Exact Match	Exact Match
2	Exact Match	Exact Match	Exact Match	Exact Match	Previous Highest
3	Exact Match	Exact Match	Exact Match	No Values	Exact Match
4	Exact Match	Exact Match	Exact Match	No Values	Previous Highest
5	Exact Match	Exact Match	No Values	No Values	Exact Match
6	Exact Match	Exact Match	No Values	No Values	Previous Highest
7	Exact Match	Exact Match	No Values	No Values	No Values
8	Exact Match	No Values	Exact Match	Exact Match	Exact Match
9	Exact Match	No Values	Exact Match	Exact Match	Previous Highest
10	Exact Match	No Values	Exact Match	No Values	Exact Match
11	Exact Match	No Values	Exact Match	No Values	Previous Highest
12	Exact Match	No Values	No Values	No Values	Exact Match
13	Exact Match	No Values	No Values	No Values	Previous Highest
14	Exact Match	Default	No Values	No Values	No Values
15	Exact Match	No Values	No Values	No Values	Default
16	Exact Match	No Values	No Values	No Values	No Values

Additional usage notes for subtemplates:

- ISC does not perform checks for the depth of subtemplates. Only one level of subtemplates is supported.
- No validations are done to check if the super template and subtemplate structure is cyclic.
- When the operator attempts to delete a subtemplate that is referenced by a super template, a warning message is generated.
- Subtemplates can be modified.
- Subtemplates can be attached to multiple super templates.
- In the current release, multiple data files are not supported for subtemplates. If multiple data files are found, the service request automatically chooses the first data file (from a list of available data files, sorted alphabetically).

Creating Data Files During Service Request Creation

The operator can create data files “on demand” during service request creation. If template(s) are attached to a service policy, and no data file(s) exist for the template(s), a wizard prompts the operator to enter values for variables. If data file(s) are created on demand during service request creation, it is possible to modify any or all of the variables during modification or re-deployment of the service request.

The service request workflow supports dynamic creation of data files as follows:

- If a template is marked as non-editable in the policy on which the service request is based, the operator cannot edit it during service request creation. However, the name of template and data files are still visible, even though they cannot be modified.
- If a template is marked as editable in the policy, then (assuming appropriate RBAC permission) the operator can change the template/data files during service request creation.
- If a template is associated with a service policy, and at least one data file exists for the template, the operator can select the appropriate data file during service request creation.
- If only one data file exists for the template, it is automatically selected.
- During service request creation, the operator can enter values for template variables.
- Optionally, if no data file exists for the template, the operator can create a new data file during service request creation. When the Datafile Chooser window is opened from Template Association window, a Create Datafile button is provided, which allows the new data file to be created.
- The Create Datafile button is only displayed if the operator has the appropriate RBAC permissions to create a data file.

See the section [Creating a Data File in the Service Request Workflow, page B-14](#) for how to set up a data file in the service request workflow.

Using Negate Templates to Decommission Template Configurations

To remove a configuration created from a template/data file, a negate template must be applied to the existing service. ISC automatically applies the appropriate negate template during the decommission of the service request. For instructions on how to use the ISC Template Manager to create negate templates, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

When a template is associated in a policy or service request, the negate template automatically gets associated. During decommission of the service, the negate template is used for deployment. When decommissioning a service request associated with a template/data file, the negate template is automatically picked up dynamically, by searching for a template name having the name of the original template followed by a suffix .Negate. This takes place at deployment time. Negate templates are dynamically instantiated based on the device attributes of the template to which it is associated.



Note

Optional attributes (such as device type, line card type, port type, and software version) applied to a template automatically apply to the corresponding negate template. The optional attributes cannot be applied directly to negate templates.

When a service is decommissioned, the appropriate negate template is deployed. The data file for a negate template is selected during deployment as follows:

- If only one data file is associated with the negate template, the data file is automatically selected.
- If multiple data files are found, the data file with same name as template is selected.
- If multiple data files are found but no data file with the same name exists, the template is skipped.
- If no data file is found, the template is skipped.

The following points cover the behavior of templates in various modification scenarios:

- If you change the template associated with a service request, the negate template automatically changes to the negate template of the newly selected template. In this case, ISC executes the negate template of the previously associated template, as well as the newly associated template.
- When a template or negate template is modified, the service request does not roll back the configuration changes made earlier through the template.
- When a service request is modified, the template command is always deployed.
- When a service request is modified without changing template/data file information, the template commands are not redeployed. The only a modification that triggers a change in template/data file results is the negation of the old template and the addition of new template commands in the device configlet.
- When a device is changed in a service request, the negate template is deployed for the old device, and the template is deployed for the new device.
- When a link in a service request is removed and a new link is added, a negate template is deployed for the deleted link and a template is deployed for the added link.

Using Templates and Data Files with Service Requests

This section describes tasks related to templates, data files, and negate templates that can be performed in the service request workflow. The following tasks are covered:

- [Choosing a Template in the Service Request Workflow, page B-12](#)
- [Creating a Data File in the Service Request Workflow, page B-14](#)
- [Decommissioning Service Requests with Added Templates, page B-15](#)
- [Viewing Templates from the Service Requests Window, page B-16](#)

Choosing a Template in the Service Request Workflow

When creating a service request, the workflow involves selecting a policy on which to base the service request, setting interface and other attributes, and so on. The specific windows and attributes presented in the workflow depend on the type of service request, such as L2VPN, VPLS, MPLS, or FlexUNI/EVC.

To associate templates and data files in a service request, you must select a link in the appropriate window of the Service Request Editor window, usually by clicking the **Add** link for the device.

Perform the following steps to choose the template(s)/data file(s) for the device(s):

Step 1 Click the **Add** link in Template/Datafile column for a device.

The Add/Remove Templates window appears.

Step 2 Click the **Add** button.

The Template Datafile Chooser window appears.

Step 3 Navigate to a template in the folder tree and select it.

The template is listed in the right side of the GUI, along with any data files that are associated with it.

At this point, you can either select an existing data file, or click the **Create Data File** button to create a data file dynamically in the workflow. The rest of the steps in this section cover the case of selecting an existing template and data file. For instructions on how to create a data file dynamically, see the section [Creating a Data File in the Service Request Workflow, page B-14](#).

Step 4 Check the check box of a data file to choose it.

Step 5 Click the **Accept** button to confirm the choice.

The template/data file combination appears in the Add/Remove Templates window.

Step 6 To add additional templates/data files to the list, click the **Add** button and repeat the appropriate steps, as covered above.

Step 7 When you are satisfied with selection of templates/data files, click the **OK** button in the Add/Remove Templates window.

The templates/data files appear in the Template/Datafile column of the Template Association window, as shown [Figure B-7](#).

Figure B-7 Sample Templates Association Window with Templates/Data Files Selected

MPLS Link Attribute Editor - Template Association

Showing 1 - 2 of 2 records

#	Device Name	Role Type	Template/Data File
1.	ce3	CE (MANAGED)	AccessList/Acl2000
2.	pe3	N-PE	AccessList1/Protocol-IP,AccessList/Acl2000

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

Note: * - Required Field

- Step 5 of 5 -

< Back Next > Finish Cancel

If multiple templates/data files are selected for a device, they appear as a comma-separated list, as shown in the figure.

Step 8 Click the **Finish** button to create the service request with the template/data file selections you chose.

If the template associated to the service request is a super template comprising of one or more subtemplates, ISC displays a message confirming this.

For information about how templates/data files are instantiated when the service is deployed, see the information provided in the section [Associating Templates to a Service Request, page B-9](#).

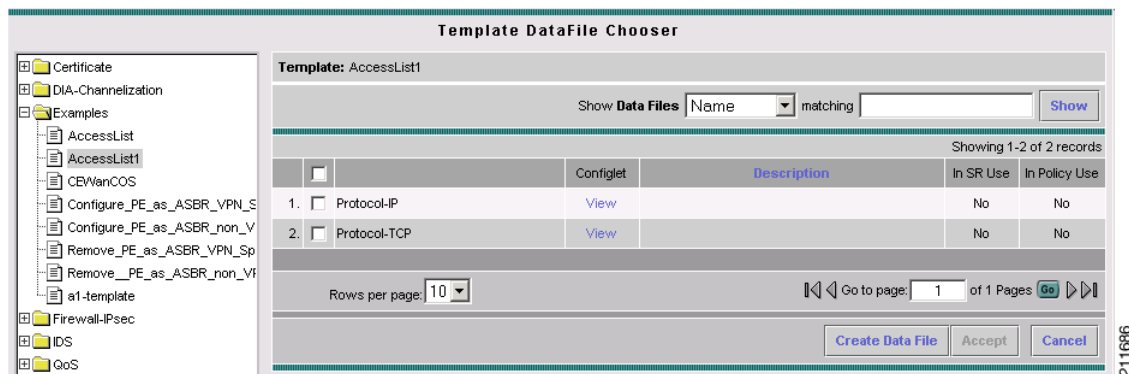
Creating a Data File in the Service Request Workflow

During the final stage of setting the link attributes for a service request, the Template Association window appears, such as the one shown in [Figure B-7](#). The Template Association window lists the devices comprising the link, the device roles, and the template(s)/data file(s) associated with the devices. You can choose the template(s)/data file(s) to be associated with the devices, as described in the section [Choosing a Template in the Service Request Workflow, page B-12](#). If one of the templates selected in the Template Datafile Chooser window does not have an associated data file or if you would like create a new data file for it, you can do this dynamically in the workflow while setting up the service request.

Perform the following steps to dynamically set up a new data file for a template:

- Step 1** In the Template Association window, click the **Add** link in the Template/Datafile column for a device. (If a template was previously selected for a device, click the link for the template name.)
The Add/Remove Templates window appears.
- Step 2** Click the **Add** button.
The Template Datafile Chooser window appears.
- Step 3** Navigate to a template in the folder tree and select it.
The template is listed in the right side of the GUI, along with any data files that are associated with it. This example uses the AccessList1 template in the Examples directory, as shown in [Figure B-8](#).

Figure B-8 Templates Datafile Chooser Window with No Data File Listed



- Step 4** Click the **Create Data File** button to create a data file dynamically in the workflow.
The Data File Editor window appears, as shown in [Figure B-9](#).

Figure B-9 Data File Editor Window

Data File Editor

General

Template: /Examples/AccessList1

Data File Name :

Description:

Variables

Application : (String)

protocol : (String)

☐ Required Fields ☐ Display Optional Variables

211687

Step 5 At this point, you are in the standard workflow for creating a data file in ISC.

In the Date File Editor window, you can specify a name and description for the data file, set variable values, view the configlet, and so on. For details on how to perform these steps, see the chapter “Service Design” in the *Cisco IP Solution Center Infrastructure Reference, 5.1*.

Step 6 When you have completed setting the attributes for the new data file, click **Save** and then **Close** to save this information and close the file; click **Configure** to show the configuration file; or click **Close** and then be sure to click **OK**, if you want to save the information you have created.

If you do not want to save this information, click **Close** and then click **Cancel**.

When the data file is saved, the Template Datafile Chooser window appears with the newly created data file listed.

Decommissioning Service Requests with Added Templates

This section describes how to decommission ISC service requests that have added templates.



Note

For general information on how templates are used in ISC, see Chapter 6, “Service Design” and Appendix D, “Template Usage” in the *Cisco IP Solution Center Infrastructure Reference, 5.1*.

As mentioned in the *Cisco IP Solution Center Infrastructure Reference, 5.1*, “Template commands are treated independently from those associated with a service creation. Consequently, template commands must be removed separately from the device(s) during a service decommission. To remove prior template commands, a separate template is needed during a decommission process. Decommissioning a service request does not automatically remove the original template commands. A separate negate template needs to be added to the decommission process and the original templates must be removed. The negate template must contain the necessary NO commands to successfully remove any unwanted IOS commands added by the original template.”

The standard way to create a service request with a template added is as follows:

1. Define the service policy.
2. Build a template with a data file (and also a negate template and data file).
3. Create the service request with the template added. The steps to do this are covered in relevant chapters of this guide.
4. Deploy the service request to which the template was added.

To decommission a deployed service request, including associated templates, you must perform the following steps.

1. Create a negate template with data file (if one does not exist). This is used to remove the commands imposed by the original template. For an explanation of negate templates, see Chapter 4, “Using Templates” in the *Cisco IP Solution Center API Programmer Guide, 5.1*.
2. Decommission the service request. The negate template will be picked up dynamically.
The service request remains in the **Requested** state, but changed to an Operation Type of Delete.
3. Deploy the service request. This decommissions the service request and downloads the negate template, which removes the original template commands.

Viewing Templates from the Service Requests Window

In the Service Requests window, a paper clip icon appears in the Data Files column if a service request has one or more templates associated with it, as shown in [Figure B-10](#).

Figure B-10 Service Requests Window with Data Files Column

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 'matching' field with an asterisk, and an 'of Type' dropdown set to 'All'. A 'Find' button is to the right. Below the search bar, it says 'Showing 1 - 4 of 5 records'. The main table has the following columns: #, Job ID, Data Files, State, Type, Operation Type, Creator, Customer Name, Policy Name, Last Modified, and Description. There are four rows of data. The first three rows have a green state icon, and the fourth row has a green state icon and a paper clip icon in the Data Files column. Below the table, there is a 'Rows per page' dropdown, a 'Go to page' field with '1' and 'of 1', and a 'Go' button. At the bottom, there is an 'Auto Refresh' checkbox checked, and a row of buttons: 'Create', 'Details', 'Status', 'Edit', 'Deploy', 'Decommission', and 'Purge'.

#	Job ID	Data Files	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	15		DEPLOYED	VRF	MODIFY	admin	Customer1	None	12/18/07 8:19 PM	
2.	16		DEPLOYED	MPLS	ADD	admin		MPLS_PE_NO_CE	12/17/07 10:49 PM	
3.	19		DEPLOYED	MPLS	MODIFY	admin		MPLS_PE_NO_CE	1/4/08 2:49 PM	
4.	21		DEPLOYED	MPLS	MODIFY	admin	Customer1	MPLS_PE_CE	1/7/08 4:23 PM	



Note

You can use the **Show Services with** field to search for service requests that have a specific data or template file. Choose **Data File Name** or **Template Name** from the drop-down list and enter a search string in the **matching** field. The matching field is not case-sensitive and supports wildcards (*). You can further limit the search by using the **of Type** field to confine the search to a particular service type. When listing service requests using Template Name, provide the entire path of the template file location (for example: examples\template, where examples is the folder name and template implies the template name).

To view the configlet(s) for the template(s) associated with a service request, perform the following steps.

- Step 1** In the Service Requests window, check the check box for a service request with an associated template, as indicated by a paper clip icon in the Data Files column.
- Step 2** Click the **Details** button.
- The Service Request Details window appears, as shown in [Figure B-11](#).

Figure B-11 Service Request Details Window

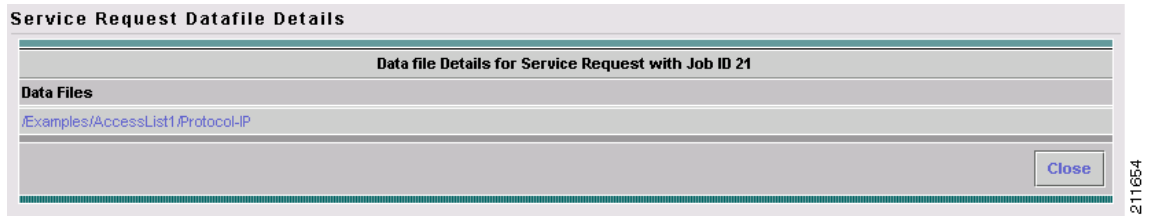
Service Request Details for Job ID 21	
Attribute	Value
Type	MPLS
State	DEPLOYED
Operation Type	MODIFY
Service Request ID	22
Last Modification Time	Mon Jan 07 16:23:33 PST 2008
Customer	Customer1
Link ID 11	
PE Name	mlpe7
PE Interface	GigabitEthernet0/1/1/0.100
CE Name	iscind-2600-2
CE Interface	FastEthernet0/0.100
VPN	VPN_1
Operation Type	MODIFY
State	DEPLOYED
Status Message	[iscind-2600-2] Audit Passed [mlpe7] Audit Passed
Associated data file(s)	/Examples/AccessList1/Protocol-IP

Links History Audit Configlets OK

The Associated data file(s) row displays a link for each data file associated with the service request, as shown in the figure.

- Step 3** Click a data file link to display the configlet for the template.
- Step 4** After viewing the configlet, click **OK** to close the configlet display window.
- Step 5** Click **OK** to close the Service Request Details window.
- Step 6** As an alternative, you can access the data files associated with a service request by clicking on the paper clip icon in the Service Requests window.

The Service Request Datafile Details window appears, as shown in [Figure B-12](#).

Figure B-12 *Service Request Datafile Details Window*

The window displays only a list of the data files associated with the service request.

- Step 7** Click a data file link to display the configlet for the template.
- Step 8** After viewing the configlet, click **OK** to close the configlet display window.
- Step 9** Click **Close** to close the Service Request Datafile Details window and return to the Service Requests window.
-



APPENDIX **C**

Troubleshooting MPLS VPNs

This chapter provides information about troubleshooting MPLS VPNs. It contains the following sections:

- [General Troubleshooting Guidelines, page C-1](#)
- [Gathering Logs for Development Engineering, page C-1](#)
- [Frequently Asked Questions, page C-2](#)

General Troubleshooting Guidelines

For general troubleshooting of failed provisioning, perform the following steps.

-
- Step 1** Identify the failed service request and go into **Details**.
- a. 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.
 - b. 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 does not give you a clear idea as to what happened, use the logs in the Task Manager to identify the problem.
- a. To do this, choose **Monitoring > Task Manager > Logs > Task Name**.
 - b. 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.
- Step 3** Also refer to the section [Frequently Asked Questions, page C-2](#) in this appendix for information on some common questions and issues.
-

Gathering Logs for Development Engineering

Go through the troubleshooting steps described in [General Troubleshooting Guidelines, page C-1](#). If you have failed to troubleshoot or identify the problem, 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.

To verify, perform the following steps.

-
- Step 1** Locate the property by choosing **Administration > Control Center**.
The Control Center Hosts page is displayed.
 - Step 2** Check 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 **Provisioning > mpls**.
 - Step 5** Click **saveDebugData**.
-

Frequently Asked Questions

Below is a list of FAQs concerning MPLS VPN provisioning.

What is the MPLS 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.

Definitions of terms mentioned in the above steps.

- **Device Configuration Service (DCS):** Responsible for uploading and downloading configuration files.
- **Generic Transport Library (GTL):** 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.

What do I do if my task does not execute even if I schedule it for immediate deployment?

This problem is likely due to one of the ISC servers being stopped or disabled.

To check the status of all ISC servers, perform the following steps.

-
- Step 1** Open the Host Configuration dialog by going to **Administration > Control Center**.
The Control Center Hosts page is displayed.
 - Step 2** Check the check box for the host of interest.
The menu buttons for the Hosts page are enabled.
 - Step 3** Choose **Servers**.
The Server Status page appears, as shown in [Figure C-1](#).

Figure C-1 *ISC Server Status*

Servers							
							Refresh
Showing 1 - 9 of 9 records							
#	☐	Name	State	Generation	Start Time	PID	Successful Heartbeats
1.	☐	cornerstonebridge	started	1	Feb 07 12:54:42 PM PST	13774	3750
2.	☐	worker	started	1	Feb 07 12:54:41 PM PST	13772	3728
3.	☐	dispatcher	started	1	Feb 07 12:54:42 PM PST	13773	3746
4.	☐	lockmanager	started	1	Feb 07 12:54:41 PM PST	13771	3733
5.	☐	nspoller	started	1	Feb 07 12:54:36 PM PST	0	3761
6.	☐	scheduler	started	1	Feb 07 12:57:07 PM PST	13798	3721
7.	☐	httpd	started	2	Feb 07 12:58:55 PM PST	13807	3752
8.	☐	dbpoller	started	1	Feb 07 12:54:36 PM PST	0	3766
9.	☐	cnsserver	started	1	Feb 07 12:54:42 PM PST	13777	3763

116287

Step 4 On the ISC server, use the **wdclient status** command to find out the detailed status of the server.

What do I do when a service request is in the Wait Deployed state?

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.

What do I do when a service request is in the Failed Audit state?

At least one command is missing on the device. Perform the following steps.

- 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.

What do I do if the service request is in the same state as it was before a deployment?

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-1](#) to find out the reason for the service request failure.

What do I do if I receive the following out-of-memory error: OutOfMemoryError?

Perform the following steps.

- Step 1** Open the Host Configuration dialog by choosing **Administration > Control Center**.
The Control Center Hosts page is displayed.

- Step 2** Check 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**.
-

What do I do if ISC will not remove a route target import/export for a VPN?

Scenario: When an MPLS service request is edited to be associated to a new VPN, the old VPN will only be removed if it is associated with only one interface. The relationship between the service request and the customer is via the VPN. The optional Customer field in a service request does not have any bearing on configuration. For example, if an MPLS service request for *custA* exists with *vpnB/cercB*, but needs to be modified to reflect *vpnA/cercA*, modifying the service request to use *vpnA/cercA* will not remove the route target for *vpnB* from the *vrfB* if there is more than one interface associated with the same VRF.

Recommended Action Running the same scenario with only one interface referring to *vrfB*, ISC will remove *vrfB* and correctly add *vrfA* with route target A.

Why does my service request go to Invalid when I choose 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.

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.

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.

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.

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.

I am 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.

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 MVRP CE.

For example, to ensure that the configlet is downloaded to the PE before it is downloaded to the CE, configure the **Provisioning.Services.mpls.DownloadWeights.weightForPE** property with a weight value greater than that of the CE.

What does the 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.

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.

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.

Why does my service request go to Invalid with the message "loopback address missing"?

This is a Layer 2 VPN question.

This is because the loopback address required to peer the pseudowire between PEs has not been defined in the PE-POP object in ISC.

What is the intent of the Allocate New Route Distinguisher check box in the MPLS policy?

There were some behavior changes implemented in ISC that differ from the legacy product "VPNSC". In VPNSC, VRFs were PE centric. Therefore, the behavior was for a new VRF to be configured for each VPN on a PE router. This behavior was modified in ISC to make VRFs VPN centric. For most of routing, the VRF/route distinguisher (RD) is only PE significant, except when doing iBGP load balancing. For this reason, it is possible to use the same values for a single VPN on all PE routers. This is more convenient for the user in context of troubleshooting, reporting, etc.

To increase flexibility for users where there is iBGP load balancing and also to address custom solutions and needs, there are two options available in ISC. One is VRF and RD Overwrite, and the other is Allocate New Route Distinguisher. VRF and RD Overwrite is exactly like it sounds. This gives the user the ability to force the VRF name and RD values for a link being provisioned. This is useful for joining a pre-existing VRF that was not provisioned by ISC. The second option, Allocate New Route Distinguisher, is only valid for configuring a new VRF and RD on a PE router for the first time. This mimics the VPNSC behavior of individual VRFs per PE router. The following is the rule for new RD when a pre-existing VPNSC repository is not involved:

When Allocate New Route Distinguisher is enabled:

- Create a new VRF if there is no matching VRF configuration on that PE.
- If there is matching VRF configuration on that PE, then reuse it.

When Allocate New Route Distinguished is disabled:

- Find the first matching VRF configuration across the whole range of PEs, regardless of the PE, if this VRF is found on the PE being configured, reuse it. If it is not found on the PE create it.
- Note: The service request might get a VRF that has already been configured on another PE router.

An issue with pre-existing VRFs that were configured under VPNSC is that in VPNSC the Allocate New Route Distinguisher flag was always turned on. Thus, when you apply the flag again, ISC first looks for an existing VRF on the PE. It uses that VRF (in this case, the one provisioned by VPNSC). If no VRF is found, ISC creates a new VRF. When adding a new link to old VPNSC links, if the Allocate New Route Distinguisher flag is not turned on, ISC finds the first matching VRF configured across the network. If the PE does not have this VRF, ISC will create it on the router.

Use cases:

1. When adding a link to an existing PE with a legacy (VPNSC) VRF, you must select the Allocate New Route Distinguisher option.
2. When adding a link to a new PE, if you desire VRF/RD values that have not been configured before in this VPN, then you must select the Allocate New Route Distinguisher option.
3. When adding a new link to a new PE, if you want to reuse a VRF/RD value that has been used elsewhere in the network, then you must select the VRF and RD Overwrite option.
4. If you provisioned a link that has incorrect VRF/RD values (that is, not matching those previously provisioned by VPNSC), the link will need to be modified and redeployed. During the modification, you must select the VRF and RD Overwrite option and specify the same VRF/RD values used in VPNSC.
5. If you are planning to deploy iBGP load balancing across multiple PEs, the Allocate New Route Distinguisher option should be always enabled. This is to make sure the condition for unique RD is met, in order to satisfy load balancing requirements.

How can an MPLS service request using standard UNI ports allow CDP packets?

By default, an MPLS service request creates MAC ACLs for a standard UNI that restricts access of BPDU handling on the Layer2 control plane. The created ACLs are similar to the following:

```
interface FastEthernet0/15
mac access-group ISC-$name in
mac access-list extended ISC-$name

deny any host 0180.c200.0000 ==> PVST, MSTP, RSTP, and STP
deny any host 0100.0ccc.cccd ==> PVST+
deny any host 0100.0ccc.cccc ==> CDP, VTP, DTP, UDLD, PAgP
deny any host 0100.0ccd.cdd0 ==> CDP,VTP,STP permit any any
```

Alternatively, when the MPLS service request is created, you can edit the link attributes and perform the following steps.

-
- Step 1** **Enable Use Existing ACL Name.**
- This will enable the Port-Based ACL Name option
- Step 2** **Enter an empty or non-existing MAC ACL name.**
-

When the MPLS service request is deployed, it will no longer issue the default BPDU filtering MAC ACLs. Instead, it will create an **access-group** command on the UNI interface that points to an empty ACL. Example:

```
interface FastEthernet0/15 mac access-group {$PACL_NAME} in
```

No MAC ACL is created.

Is it possible to use 2 or 3 address pools when creating an L3 VPN?

Imagine that you have IP pool 10.10.10.0/24 assigned to a region, and a PE is assigned to this region. What if one customer is using the same subnet in his LAN range? This forces you to use another subnet for the PE-CE link. How is this handled by ISC? The only way is to do it manually, without using auto pick. ISC does not support for the use of different address pools for different customers.

Another related issue is as follows. If a customer is using the same IP addresses inside his LAN segment as are used in the ISC pool of IP addresses, this causes a problem. For this reason, you must have multiple subnets for the PE-CE IP addresses, and use the suitable one (one that does not conflict with the IP addresses used by the customer). When you create an IP address pool, the repository knows the range, and will not allow you to use overlapping IP addresses as part of the pool. ISC does not have any support for different pools to be used within the same PE. ISC allows you to create multiple pools, but you can only use one based on the provider region. ISC picks up the next in line if the first pool runs out of IP addresses. There is no selection mechanism for you to select which pool will be used with auto pick. You can use manually added IP addresses, as long as the IP address do not overlap with the pool.

When will an IP address from the MPLS IP address pool be returned to the available pool after the service request is decommissioned?

When a service request is decommissioned, the IP address is returned back to the available pool after the service request goes to the DEPLOYED state. ISC prevents reuse of the returned IP addresses by a new service request for about twenty-four hours. The same behavior applies when the service request is decommissioned and then purged.

Why doesn't ISC remove some of the router BGP/EIGRP commands when a service request is decommissioned?

ISC removes the address family CLIs from router BGP or EIGRP configurations if and only if the VRF is removed. For router EIGRP, the process is not removed due to the potential presence of other CLIs that were not configured by ISC. This is particularly applicable when the network statement was added outside of ISC. ISC does not remove the redistribution from other routing protocols under EIGRP because the redistribute command might not be created specifically for the link.

ISC only removes the router OSPF process if the VRF is removed. This applies only for a PE. For a CE, router OSPF is removed if the network statement is removed. ISC does not remove router BGP nor router EIGRP.

What happens if the platform or IOS version does not support Q-in-Q (for example WS-X6724-SFP)?

The service request will result in a Failed Deploy state, and the log file will be similar to:

```
SEVERE Provisioning.ProvDrvDownload failed for device NPE-1: 315 : Error downloading
cmd=[encapsulation dot1q 158 second-dot1q 1510], response=[encapsulation dot1q 158
second-dot1q 1510^
```

```
% Invalid input detected at '^' marker.NPE-1(config-subif)#]
```

Edit the service request, disable second VLAN ID, and then re-deploy.

Why doesn't ISC provision Q-in-Q, although the hardware/IOS does support Q-in-Q?

Possible errors:

- The port is in switchport mode. Solution: Check the port configuration, and if necessary, run **no switchport**.
- The SVI flag is enabled. Solution: Disable SVI.

Why does a port with existing subinterfaces (Q-in-Q) plus SVI on same interface result in INVALID?

This is a multiplexed user-to-network interface (MUX-UNI) service example. ISC 5.1 does not support MUX-UNI. There is a workaround in place, but requires approval before being implemented at a customer site. Please contact isc-mktg@cisco.com.

An example error output in the ISC log follows:

```
EngineError: layer 3 sub interface exists for this port. To proceed, delete the sub  
interface first.functionElement: provision multihopdeviceElement:  
LogicalLinkconfigElement: logical linkscontext: MplsVpnLink, ID: 77
```

Is it possible to deploy single dot1q and Q-in-Q service requests under the same interface/port?

Yes.

How can I remove the second VLAN ID from a service request that is Deployed with Q-in-Q?

You must edit/modify the service request, remove the second VLAN ID entry, and redeploy the service request. A configlet like the following will be created:

```
interface GigabitEthernet2/0/15.158  
no encapsulation dot1Q  
encapsulation dot1Q 158  
ip address 10.1.1.105 255.255.255.252
```




APPENDIX D

Service Request Transition States

This appendix documents service request transition states.

[Table D-1](#) and [Table D-2 on page D-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 D-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 D-1](#) shows the service request transitions from *Requested* to *Lost*.

Table D-1 State Transition Paths for ISC Service Requests (Part 1)

Service Request States	Requested	Pending	Failed Audit	Deployed	Functional	Lost
Requested	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
Pending	No transition to Requested	Successful service request deployment	Audit is not successful	Audit is successful	Routing audit is successful	No transition to Lost
Failed Audit	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	No transition to Lost
Deployed	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	Audit found error
Functional	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	No transition to Deployed	Routing audit is successful	Audit found error
Lost	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Audit is successful	Routing audit is successful	Audit found error
Broken	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 D-1 State Transition Paths for ISC Service Requests (Part 1) (continued)

Service Request States	Requested	Pending	Failed Audit	Deployed	Functional	Lost
Invalid	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
Failed Deploy	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
Closed	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 D-2 shows the service request transitions from *Broken* to *Closed*.

Table D-2 State Transition Paths for ISC Service Requests (Part 2)

Service Request States	Broken	Invalid	Failed Deploy	Closed
Requested	No transition to Broken	Deploy service request error	Deployment failed	No transition to Closed
Pending	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
Failed Audit	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
Deployed	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
Functional	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
Lost	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
Broken	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
Invalid	No transition to Broken	Redeployment caused service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed

Table D-2 *State Transition Paths for ISC Service Requests (Part 2) (continued)*

Service Request States	Broken	Invalid	Failed Deploy	Closed
Failed Deploy	No transition to Broken	Redeploy service request error	Redeployment service request failed. Configlet cannot be downloaded.	No transition to Closed
Closed	No transition to Broken	No transition to Invalid	No transition to Failed Deploy	No transition to Closed



APPENDIX **E**

MPLS VPN Concepts

This appendix provides conceptual information useful for understanding MPLS. It contains the following sections:

- [MPLS VPNs, page E-1](#)
- [MPLS VPN Security, page E-8](#)

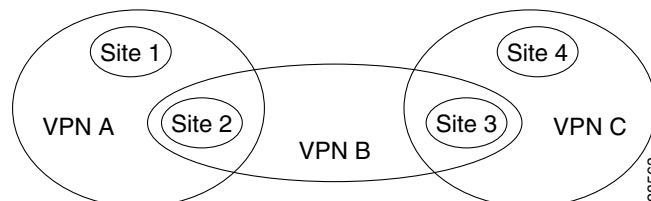
MPLS VPNs

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 an MPLS VPN, the 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 E-1 *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 E-3.

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 (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
```

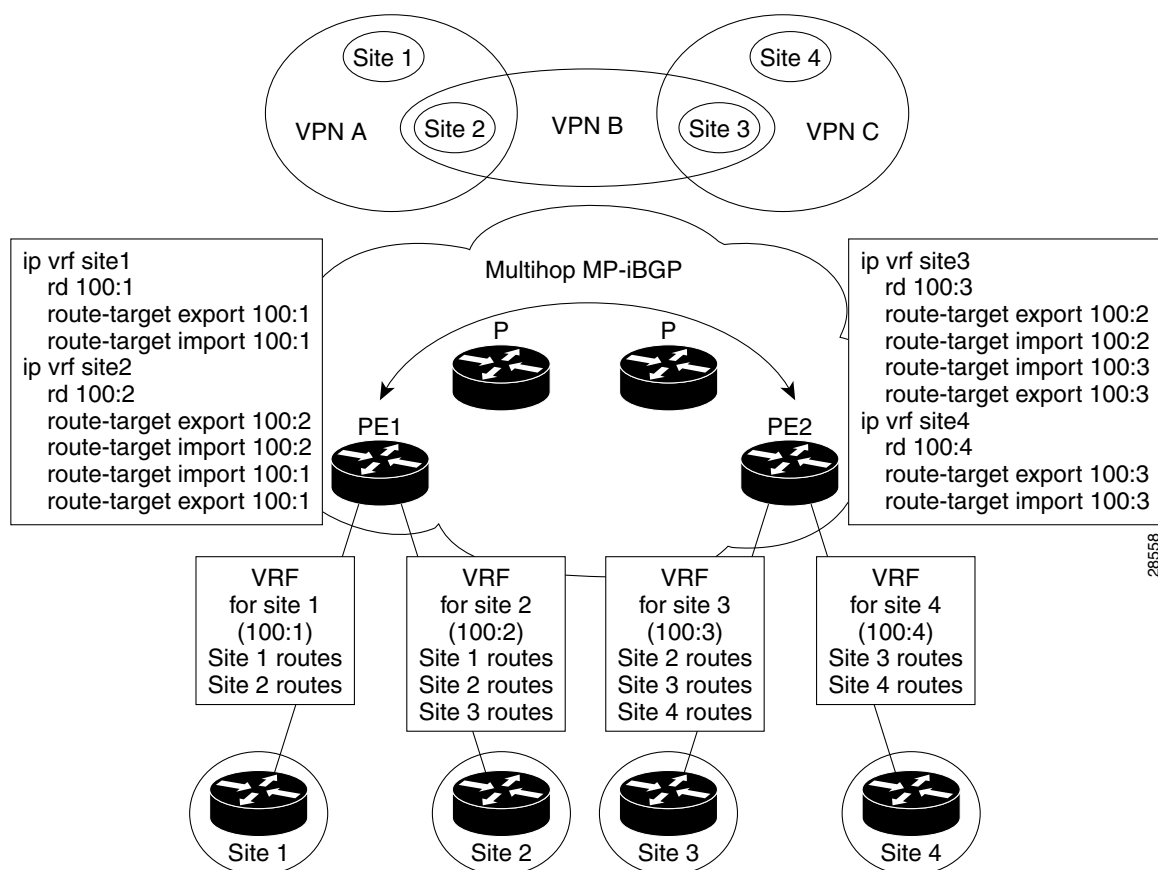
A VRF for an extranet VPN topology in the Green VPN would be called:

```
ip vrf V1:green-etc
```

Thus, you can read the VPN name and the topology type directly from the name of the VRF.

[Figure E-2](#) 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 E-2 VRFs for Sites in Multiple VPNs



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# configure terminal Router(config)#	Enter global configuration mode.
Step 2	Router(config)# ip vrf vrf_name	For example, ip vrf CustomerA 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)# rd RD_value	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)# route-target import export both community	Enter the route-target information for the VRF.

Independent VRF Object Management

ISC allows you to specify VPN and VRF information in an independent VRF object, which is subsequently deployed to a PE device and then associated with an MPLS VPN link via an MPLS VPN service request. For details on using this feature, see [Chapter 3, “Independent VRF Management.”](#)

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 choose 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 2-32).

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.

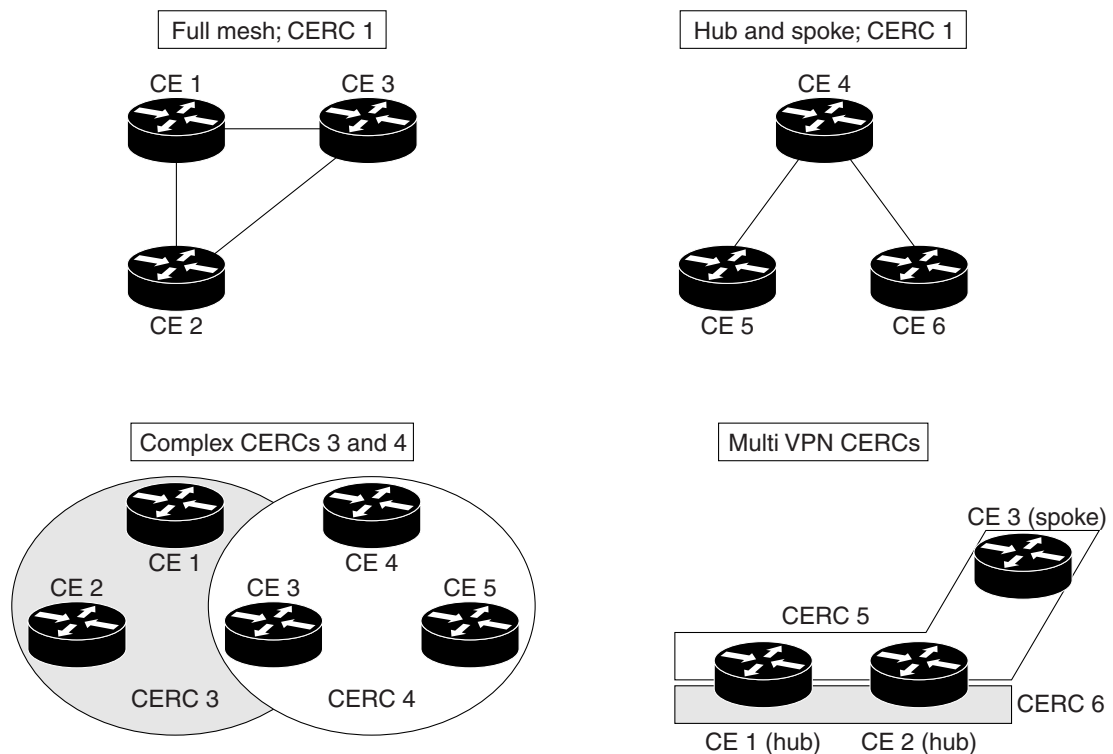
Whenever you create a VPN, the ISC software creates one default CERC for you. This means that until you need advanced customer layout methods, you will not need to define new CERCs. Up to that point, you can think of a CERC as standing for the VPN itself—they are one and the same. If, for any reason, 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 2-32](#)).

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 E-3](#) shows several examples of the topologies that IP Solution Center CERCs can employ.

Figure E-3 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.



Note

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 want to use the Internet to his upstream or peer providers.

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.

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 and hiding the IP addresses in the MPLS core.

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.

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 exits 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, we recommend 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.

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 E-5](#)).

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 because each VPN has a unique identifier.

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.



INDEX

Numerics

6VPE

- IPv6 and 6VPE support in MPLS VPN [4-1](#)
- overview [4-1](#)

A

access domains

- creating [2-12](#)
- management [12-11](#)

access ports [12-11](#)

addresses

- address space and routing separation [E-8](#)
- address space separation [E-8](#)
- IP addresses [5-2](#)

address pools, creating IPv4 address pools [2-16](#)

auditing

- configuration audit [6-29](#)
- MPLS VPN service requests [4-11](#)
- performing a configuration audit [6-30](#)
- performing a functional audit [6-28](#)
- service requests [6-28](#)
- where to find a configuration audit [6-30](#)
- where to find a functional audit [6-29](#)
- why a configuration audit could fail [6-30](#)
- why a functional audit could fail [6-29](#)

authentication [E-13](#)

autonomous systems

- benefits [13-2](#)
- exchanging VPN routing information [13-4](#)
- overview [13-1](#)
- routing between autonomous systems [13-3](#)

routing between subautonomous systems in a confederation [13-8](#)

spanning multiple autonomous systems [13-1](#)

using ISC to span multiple autonomous systems [13-9](#)

using templates to support inter-autonomous system solutions [13-11](#)

B

BGP

multipath load sharing and maximum path configuration [5-32](#)

protocol [5-18](#)

removing a multipath configuration [5-34](#)

C

cable services

- benefits of cable MPLS VPNs [10-1](#)
- cable MPLS VPN network [10-2](#)
- cable VPN configuration overview [10-4](#)
- cable VPN interfaces and subinterfaces [10-5](#)
- creating a cable subinterface service request [10-6](#)
- creating cable link service requests [10-10](#)
- creating the service requests [10-6](#)
- management VPN in the cable network [10-3](#)
- overview of MPLS VPN cable services [10-1](#)
- provisioning cable services [10-1](#)
- provisioning cable services in ISC [10-5](#)

carrier supporting carrier (see CSC) [11-1](#)

CERCs, creating [2-32](#)

CE routing communities (see CERCs) [E-6](#)

- CEs
 - defining a CE as an MCE [9-8](#)
 - giving only default routes to CE [5-12](#)
 - managed CE routers [9-2](#)
 - specifying interface parameters [5-4](#)
 - unmanaged CE routers [9-1](#)
- CLEs, adding a CLE to a service request [6-25](#)
- configlet examples
 - CE-PE L3 MPLS VPN [A-7](#)
 - CE-PE L3 MPLS VPN (BGP with full-mesh) [A-5](#)
 - CE-PE L3 MPLS VPN (BGP with SOO) [A-6](#)
 - CE-PE L3 MPLS VPN (Q-in-Q/Second VLAN ID) [A-16](#)
 - L2 Access into L3 MPLS VPN [A-3](#)
 - N-PE L3 MPLS VPN (IPv4, IOS XR, OSPF) [A-8](#)
 - N-PE L3 MPLS VPN (IPv6, IOS XR, EIGRP) [A-12](#)
- configlets
 - overview [A-1](#)
 - sample configlets [A-1](#)
 - viewing configlets generated by a service request [6-31](#)
 - viewing configlets generated by the MPLS VPN service request [6-13](#)
 - viewing configlets on IOS XR devices [6-32](#)
 - VRF-related configlets [4-4](#)
- configuration audit [6-29](#)
 - performing a configuration audit [6-30](#)
 - where to find a configuration audit [6-30](#)
 - why a configuration audit could fail [6-30](#)
- configuration files, editing [6-33](#)
- configurations, collecting [2-4](#)
- configuring, ETTH [12-12](#)
- copying, VRF objects [3-5](#)
- CPEs, creating [2-8](#)
- creating
 - access domains [2-12](#)
 - cable link service requests [10-10](#)
 - cable subinterface service requests [10-6](#)
 - CERCs [2-32](#)
 - CPEs [2-8](#)
 - customers [2-8](#)
 - custom reports [14-7](#)
 - device groups [2-6](#)
 - devices [2-2](#)
 - IPv4 address pools [2-16](#)
 - logical devices [2-3](#)
 - MCE service requests [9-10](#)
 - MPLS VPN PE-CE service requests [7-8](#)
 - MPLS VPNs [2-22](#)
 - multicast pools [2-16](#)
 - multicast VPNs [2-26](#)
 - MVRFCE PE-CE service policies [8-4](#)
 - MVRFCE PE-CE service requests [8-8](#)
 - MVRFCE PE-noCE service requests [8-14](#)
 - new VRF objects [3-2](#)
 - PE-CE service policies [7-4](#)
 - PE-CE service requests [7-8](#)
 - PE-noCE service policies [7-6, 8-6](#)
 - PE-noCE service requests [7-12](#)
 - PEs [2-11](#)
 - providers [2-10](#)
 - regions [2-11](#)
 - resource pools [2-15](#)
 - route distinguisher pools [2-17](#)
 - route target pools [2-18](#)
 - site of origin pools [2-19](#)
 - sites [2-8](#)
 - unmanaged MVRFCEs [8-19](#)
 - VC ID pools [2-20](#)
 - VLAN pools [2-21](#)
 - VPNs [2-22](#)
- CSC
 - backbone network with BGP/MPLS VPN service provider customer carrier [11-3](#)
 - backbone network with ISP customer carrier [11-1](#)
 - defining CSC service policies [11-5](#)
 - IPv4 BGP label distribution [11-4](#)
 - ISC configuration options [11-4](#)
 - LDP/IGP [11-4](#)

- overview [11-1](#)
- provisioning [11-1, 11-5](#)
- service requests [11-5](#)
- support for [5-12](#)

customers, creating [2-8](#)

D

data files

- creating a data file in the service request workflow [B-14](#)
- creating data files during service request creation [B-10](#)

defining

- CSC service policies [11-5](#)
- MPLS VPN service policies [5-2](#)
- VPN for the PE-CE link [7-3](#)
- VPNs [2-22](#)
- VRF and VPN information [5-29](#)
- VRF service requests [3-11](#)

deleting

- VRF objects [3-10](#)
- VRF service requests [3-14](#)

deploying

- service requests [6-25](#)
- VRF service requests [3-13](#)

device groups, creating [2-6](#)

devices

- creating [2-2](#)
- creating logical devices [2-3](#)
- how ISC accesses network devices [6-5](#)
- setting up for IOS XR support [2-6](#)

E

editing

- configuration files [6-33](#)
- multi-VRF edit mode [3-7](#)
- PEs [2-12](#)

- service policies [5-1](#)
- single-VRF edit mode [3-7](#)

EIGRP, protocol [5-24](#)

encapsulation

- interface types and their corresponding encapsulations [5-6](#)

Ethernet-to-the-home (see ETTH) [12-9](#)

ETTH

- configuring [12-12](#)
- implementation [12-11](#)

F

full mesh, configurations [E-8](#)

functional audit [6-28](#)

- performing a functional audit [6-28](#)
- where to find a functional audit [6-29](#)
- why a functional audit could fail [6-29](#)

H

hub and spoke, configurations [E-7](#)

I

IGM, with MVR [12-11](#)

independent VRF management [3-1](#)

independent VRF management, overview of [3-1](#)

inter-AS

- 10B hybrid model [13-11](#)
- creating templates for [13-12](#)
- RT-rewrite [13-12](#)

interfaces

- interface types and their corresponding encapsulations [5-6](#)

intranets and extranets [E-2](#)

IOS

- comparison of IOS and IOS XR [4-3](#)
- comparison of IOS and IOS XR device configlets [4-3](#)

IOS XR

- comparison of IOS and IOS XR [4-3](#)
- comparison of IOS and IOS XR device configlets [4-3](#)
- multicast routing on IOS XR devices [4-6](#)
- viewing configlets on IOS XR devices [6-32](#)

IP addresses [5-2](#)

- resolution of [E-15](#)
- specifying the IP address scheme [5-8](#)

IPv4, routing information [6-14](#)

IPv6 [4-1](#)

- interface-related configlets [4-4](#)
- inventory and device management [4-7](#)
- IPv6 and 6VPE features not supported in ISC 5.0.1 [4-11](#)
- IPv6 and 6VPE support in MPLS VPN [4-1](#)
- ISC and MPLS VPN updates to support IPv6 and 6VPE [4-7](#)
- overview [4-1](#)
- routing information [6-15](#)
- using EIGRP as the PE-CE routing protocol [4-5](#)
- using OSPF as the PE-CE routing protocol [4-4](#)
- using static as the PE-CE routing protocol [4-5](#)
- VPN creation and configuration [4-8](#)
- VPN provider edge router (6VPE) [4-2](#)
- VRF object support [4-8](#)

ISC

- overview of services [2-1](#)
- service activation [1-1](#)
- setting up services for [2-1](#)

L

label spoofing [E-12](#)

LDP authentication [E-13](#)

links

- adding PE-CE links to management VPNs [9-14](#)
- defining a VPN for the PE-CE link [7-3](#)
- MPLS VPN PE-CE link overview [7-1](#)
- MVRFCE PE-CE link overview [8-1](#)

provisioning multi-VRFCE PE-CE links [8-1](#)

provisioning regular PE-CE links [7-1](#)

logs

- monitoring task logs [2-5](#)
- used in troubleshooting [C-1](#)

loopback, using existing loopback interface number [5-10](#)

M

management networks

- advantages of [9-6](#)
- defining CE as MCE [9-8](#)
- implementation techniques [9-4](#)
- management CE (MCE) [9-5](#)
- management PE (MPE) [9-5](#)
- management VPN [9-5](#)
- out-of-band technique [9-7](#)
- overview [9-1](#)
- provisioning a management CE in ISC [9-8](#)
- subnets [9-3](#)

maximum path, BGP multipath load sharing and maximum path configuration [5-32](#)

MCEs

- creating MCE service requests [9-10](#)
- defining a CE as an MCE [9-8](#)

modifying

- deployed VRF objects [3-9](#)
- non-deployed VRF objects [3-7](#)
- VRF service requests [3-14](#)

monitoring

- service requests [6-27](#)
- task logs [2-5](#)

MP-BGP security features [E-14](#)

MPLS reports (see reports) [14-1](#)

MPLS VPNs [4-9](#)

- concepts [E-1](#)
- creating [2-22](#)
- getting started [1-1](#)
- overview of MPLS VPN cable services [10-1](#)

- policies [1-2](#)
- prerequisites [1-1](#)
- prerequisite tasks [7-2](#)
- reports [4-11](#)
- security [E-8](#)
- service policies [5-1](#)
- service provisioning [4-9](#)
- service request auditing [4-11](#)
- service requests [1-2, 6-1](#)
- service requests (see also service requests) [4-10](#)
- topology example [6-6](#)

multicast, creating multicast VPNs [2-26](#)

multicast pools, creating [2-16](#)

multicast routing, on IOS XR devices [4-6](#)

multipath

- BGP multipath load sharing and maximum path configuration [5-32](#)
- removing a multipath configuration [5-34](#)

multi-VRF, creating a service request for [6-15](#)

multi-VRFCEs (see MVRFCEs) [8-1](#)

MVRFCEs

- creating an unmanaged MVRFCE [8-19](#)
- creating MVRFCE PE-CE service policies [8-4](#)
- creating MVRFCE PE-CE service requests [8-8](#)
- creating MVRFCE PE-noCE service requests [8-14](#)
- defining VPN for MVRFCE PE-CE links [8-3](#)
- MVRFCE PE-CE link overview [8-1](#)
- prerequisite tasks for [8-3](#)
- provisioning MVRFCE PE-CE links [8-1](#)

N

negate templates (see templates) [B-11](#)

networks

- backbone networks with BGP/MPLS VPN service provider customer carrier [11-3](#)
- backbone networks with ISP customer carrier [11-1](#)
- full mesh [E-8](#)
- hub and spoke [E-7](#)

- label spoofing [E-12](#)
- management network subnets [9-3](#)
- overview of the ISC management network [9-1](#)
- resistance to attacks [E-10](#)
- topology [7-2, 8-2](#)

NPC ring topology [12-1](#)

- configuring [12-5](#)
- creating ring of three PE-CLEs [12-2](#)
- overview [12-1](#)

O

OSPF, protocol [5-21](#)

out-of-band technique [9-7](#)

P

PEs

- creating [2-11](#)
- creating a PE-only service request [6-20](#)
- editing [2-12](#)
- specifying interface parameters [5-4](#)

prerequisites, for MPLS VPN [7-2](#)

protocols

- BGP [5-18](#)
- EIGRP [5-24](#)
- for cable services [5-28](#)
- OSPF [5-21](#)
- RIP [5-14](#)
- setting static routing protocol Attributes (for IPv4 and IPv6) [6-13](#)
- static protocol chosen [5-12](#)

providers, creating [2-10](#)

provisioning

- cable services [10-1](#)
- cable services in ISC [10-5](#)
- CSC [11-1](#)
- management CEs in ISC [9-8](#)
- management VPN [9-1](#)

multiple devices [12-1](#)
 MVRFC PE-CE links [8-1](#)
 regular PE-CE links [7-1](#)
 PVLAN (protected ports) [12-11](#)

Q

Q-in-Q, usage notes [6-10](#)

R

regions, creating [2-11](#)
 reports
 6VPE supported devices report [14-6](#)
 accessing MPLS reports [14-1](#)
 creating custom reports [14-7](#)
 generating MPLS reports [14-1](#)
 MPLS PE service report [14-3](#)
 MPLS service request report [14-4](#)
 MPLS service request report - 6VPE [14-5](#)
 MPLS VPNs [4-11](#)
 overview [14-1](#)
 running reports [14-2](#)
 residential service [12-15](#)
 policy for residential services over shared VLAN [12-16](#)
 resource pools [4-9](#)
 creating [2-15](#)
 overview [2-15](#)
 ring topology (see NPC ring topology) [12-1](#)
 RIP, protocol [5-14](#)
 route distinguisher pools, creating [2-17](#)
 route distinguishers [E-5](#)
 routes
 giving only default routes to CE [5-12](#)
 redistribution of IP routes [5-12](#)
 route target communities [E-6](#)
 route target pools, creating [2-18](#)
 route targets [E-5](#)

routing
 authentication [E-13](#)
 IPv4 routing information [6-14](#)
 IPv6 routing information [6-15](#)
 separation [E-9](#)
 routing protocols
 securing [E-10](#)
 specifying the routing protocol for a service [5-11](#)

S

searching
 for VRF objects in the ISC repository [3-7](#)
 for VRF service requests [3-15](#)
 Second VLAN ID, usage notes [6-10](#)
 security
 address space and routing separation [E-8](#)
 address space separation [E-8](#)
 ensuring VPN isolation [E-15](#)
 hiding the MPLS core structure [E-9](#)
 IP address resolution [E-15](#)
 label spoofing [E-12](#)
 LDP authentication [E-13](#)
 MP-BGP security features [E-14](#)
 of MPLS VPNs [E-8](#)
 PE-CE interface [E-12](#)
 resistance to attacks [E-10](#)
 routing authentication [E-13](#)
 routing separation [E-9](#)
 securing the MPLS core [E-12](#)
 securing the routing protocol [E-10](#)
 separation of CE-PE links [E-13](#)
 trusted devices [E-12](#)
 service activation of ISC [1-1](#)
 service policies [4-9](#)
 associating templates and data files to a policy [B-4](#)
 associating templates with [5-34](#)
 creating a PE-CE service policy [7-4](#)
 creating a PE-noCE service policy [7-6](#)

- creating MPLS VPN PE-CE service policies [7-3](#)
- creating MVRFCE PE-CE service policies [8-4](#)
- creating PE-noCE service policies [8-6](#)
- CSC [11-5](#)
- defining [5-2](#)
- editing [5-1](#)
- MPLS VPN [4-9](#)
- MPLS VPNs [5-1](#)
- overview [5-1](#)
- PE-CE service policy overview [7-3](#)
- service provisioning, MPLS VPN [4-9](#)
- service requests
 - adding a CLE to a service request [6-25](#)
 - associating templates and data files to a service request [B-9](#)
 - auditing [6-28](#)
 - cable services [10-6](#)
 - creating a cable subinterface service request [10-6](#)
 - creating a multi-VRF service request [6-15](#)
 - creating an MPLS VPN PE-CE service request [6-7](#)
 - creating a PE-only service request [6-20](#)
 - creating cable link service requests [10-10](#)
 - creating data files during service request creation [B-10](#)
 - creating MCE service requests [9-10](#)
 - creating MPLS VPN PE-CE service requests [7-8](#)
 - creating MVRFCE PE-CE service requests [8-8](#)
 - creating MVRFCE PE-noCE service requests [8-14](#)
 - creating PE-CE service requests [7-8](#)
 - creating PE-noCE service requests [7-12](#)
 - CSC [11-5](#)
 - decommissioning service requests with templates [B-15](#)
 - deploying [6-25](#)
 - examples of creating MPLS VPN service requests [6-6](#)
 - monitoring [6-27](#)
 - MPLS VPNs [4-10, 6-1](#)
 - overview [6-1](#)
 - provisioning using a unique route distinguisher [2-29](#)

- residential services [12-18](#)
- state transition paths for ISC service requests [D-1](#)
- summary of states [6-3](#)
- transition states [6-1, D-1](#)
- user operations on [6-4](#)
- viewing configlets generated by a service request [6-31](#)
- viewing configlets generated by the MPLS VPN service request [6-13](#)
- services, enhancements for [6-5](#)
- setting up, devices for IOS XR support [2-6](#)
- site of origin pools, creating [2-19](#)
- sites, creating [2-8](#)
- specifying
 - IP address scheme [5-8](#)
 - PE and CE interface parameters [5-4](#)
 - routing protocol for a service [5-11](#)
- states, transitions of [6-1](#)
- static
 - setting static routing protocol Attributes (for IPv4 and IPv6) [6-13](#)
 - static protocol [5-12](#)
- subtemplates (see templates) [B-10](#)

T

- templates
 - associating subtemplates during service provisioning [B-9](#)
 - associating templates and data files to a policy [B-4](#)
 - associating templates to a service request [B-9](#)
 - choosing a template in the service request workflow [B-12](#)
 - creating inter-AS templates [13-12](#)
 - decommissioning service requests with added templates [B-15](#)
 - decommissioning service requests with added templates. [B-15](#)
 - default subtemplate matching criteria [B-10](#)
 - enabling for policies [5-34](#)
 - overview [B-1](#)

- overview of template support in ISC policies [B-4](#)
- overview of template use in service requests [B-8](#)
- summary of template manager features [B-1](#)
- template and data file workflow [B-3](#)
- using negate templates to decommission template configurations [B-11](#)
- using templates and data files with service requests [B-12](#)
- using templates to support inter-autonomous system solutions [13-11](#)
- using templates with ISC policies [B-4](#)
- using templates with service requests [B-8](#)
- viewing templates from the service requests window [B-16](#)
- working with templates and data files [B-1](#)

topology

- example of MPLS VPN topology [6-6](#)
- networks [8-2](#)
- network topology [7-2](#)

transition states of service requests [D-1](#)

troubleshooting

- frequently asked questions [C-2](#)
- gathering logs [C-1](#)
- general troubleshooting guidelines [C-1](#)
- MPLS VPNs [C-1](#)

trusted devices [E-12](#)

U

unique route distinguisher, enabling for a VPN [2-28](#)

unique route distinguisher, using to provision service requests [2-29](#)

V

VC ID pools, creating [2-20](#)

VLAN ID, usage notes [6-10](#)

VLAN pools, creating [2-21](#)

VPN routing and forwarding tables (see also VRFs) [E-3](#)

VPNs

- adding PE-CE links to management VPNs [9-14](#)
- benefits of cable MPLS VPNs [10-1](#)
- connectivity between VPNs [E-13](#)
- creating [2-22](#)
- creating and configuring on IPv6 devices [4-8](#)
- defining [2-22](#)
- defining a VPN for the PE-CE link [7-3](#)
- defining VRF and VPN information [5-29](#)
- enabling a unique route distinguisher for a VPN [2-28](#)
- ensuring VPN isolation [E-15](#)
- issues regarding access to VPNs [9-4](#)
- provisioning management VPN [9-1](#)
- troubleshooting [C-1](#)
- VPN routing and forwarding tables [E-3](#)

VRFs

- copying a VRF object [3-5](#)
- creating a new VRF object [3-2](#)
- decommissioning and deleting VRF service requests [3-14](#)
- defining VRF and VPN information [5-29](#)
- defining VRF service requests [3-11](#)
- deleting VRF objects [3-10](#)
- deleting VRF objects associated with VRF service requests [3-10](#)
- deploying VRF service requests [3-13](#)
- implementation [E-4](#)
- independent VRF management [3-1](#)
- independent VRF object management [E-5](#)
- migrating existing MPLS VPN service requests to the VRF object model [3-21](#)
- modifying deployed VRF objects [3-9](#)
- modifying non-deployed VRF objects [3-7](#)
- modifying VRF service requests [3-14](#)
- multi-VRF edit mode [3-7](#)
- overview of VRF service requests [3-11](#)
- relationship of VRF object and service requests and PE device [3-16](#)
- searching for MPLS VPN service requests by VRF object name [3-20](#)

- searching for VRF objects in the ISC repository [3-7](#)
- searching for VRF service requests by VRF object name [3-15](#)
- single-VRF edit mode [3-7](#)
- specifying VRF objects within MPLS VPN service policies [3-20](#)
- specifying VRF objects within MPLS VPN service requests [3-16](#)
- using a VRF object in an MPLS service request [3-20](#)
- using VRFs with MPLS VPN service requests and policies [3-16](#)
- viewing the configlet generated by a deployed VRF service request [3-15](#)
- VRF instance [E-5](#)
- VRF object support for IPv6 [4-8](#)
- VRF-related configlets [4-4](#)
- working with VRF objects [3-2](#)
- working with VRF service requests [3-11](#)

