



Cisco IOS Multiprotocol Label Switching Configuration Guide

Release 12.4

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, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

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.

Cisco IOS Multiprotocol Label Switching Configuration Guide
© 2008 Cisco Systems, Inc. All rights reserved.



About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page ii](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xi](#)

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
Courier font	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
 - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
 - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/all_release/all_mcl.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xi](#).

Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1 *Cisco IOS and Cisco IOS XE Configuration Guides and Command References*

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS AppleTalk Configuration Guide</i>	AppleTalk protocol.
<i>Cisco IOS XE AppleTalk Configuration Guide</i>	
<i>Cisco IOS AppleTalk Command Reference</i>	
<i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
<i>Cisco IOS Asynchronous Transfer Mode Command Reference</i>	

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<p><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></p> <p><i>Cisco IOS Bridging Command Reference</i></p> <p><i>Cisco IOS IBM Networking Command Reference</i></p>	<ul style="list-style-type: none"> • Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
<p><i>Cisco IOS Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS XE Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS Broadband and DSL Command Reference</i></p>	<p>Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).</p>
<p><i>Cisco IOS Carrier Ethernet Configuration Guide</i></p> <p><i>Cisco IOS Carrier Ethernet Command Reference</i></p>	<p>Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).</p>
<p><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS Configuration Fundamentals Command Reference</i></p>	<p>Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.</p>
<p><i>Cisco IOS DECnet Configuration Guide</i></p> <p><i>Cisco IOS XE DECnet Configuration Guide</i></p> <p><i>Cisco IOS DECnet Command Reference</i></p>	<p>DECnet protocol.</p>
<p><i>Cisco IOS Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS XE Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS Dial Technologies Command Reference</i></p>	<p>Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).</p>
<p><i>Cisco IOS Flexible NetFlow Configuration Guide</i></p> <p><i>Cisco IOS Flexible NetFlow Command Reference</i></p>	<p>Flexible NetFlow.</p>

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS H.323 Configuration Guide</i>	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
<i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS XE High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i>	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<i>Cisco IOS Integrated Session Border Controller Command Reference</i>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
<i>Cisco IOS Intelligent Service Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Service Gateway Command Reference</i>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS XE Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS XE IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS XE IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS XE IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS XE IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i>	Cisco IOS IP Service Level Agreements (IP SLAs).
<i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS XE IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS XE IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i>	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
<i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS XE ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i>	ISO connectionless network service (CLNS).
<i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS XE LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i>	Cisco IOS radio access network products.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<p><i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></p>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<p><i>Cisco IOS Multi-Topology Routing Configuration Guide</i></p> <p><i>Cisco IOS Multi-Topology Routing Command Reference</i></p>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<p><i>Cisco IOS NetFlow Configuration Guide</i></p> <p><i>Cisco IOS XE NetFlow Configuration Guide</i></p> <p><i>Cisco IOS NetFlow Command Reference</i></p>	Network traffic data analysis, aggregation caches, export features.
<p><i>Cisco IOS Network Management Configuration Guide</i></p> <p><i>Cisco IOS XE Network Management Configuration Guide</i></p> <p><i>Cisco IOS Network Management Command Reference</i></p>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
<p><i>Cisco IOS Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS XE Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS Novell IPX Command Reference</i></p>	Novell Internetwork Packet Exchange (IPX) protocol.
<p><i>Cisco IOS Optimized Edge Routing Configuration Guide</i></p> <p><i>Cisco IOS Optimized Edge Routing Command Reference</i></p>	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
<p><i>Cisco IOS Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS Quality of Service Solutions Command Reference</i></p>	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
<p><i>Cisco IOS Security Configuration Guide</i></p> <p><i>Cisco IOS XE Security Configuration Guide</i></p> <p><i>Cisco IOS Security Command Reference</i></p>	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Service Selection Gateway Configuration Guide</i> <i>Cisco IOS Service Selection Gateway Command Reference</i>	Subscriber authentication, service access, and accounting.
<i>Cisco IOS Software Activation Configuration Guide</i> <i>Cisco IOS Software Activation Command Reference</i>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<i>Cisco IOS Software Modularity Installation and Configuration Guide</i> <i>Cisco IOS Software Modularity Command Reference</i>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
<i>Cisco IOS Terminal Services Configuration Guide</i> <i>Cisco IOS Terminal Services Command Reference</i> <i>Cisco IOS XE Terminal Services Command Reference</i>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<i>Cisco IOS Virtual Switch Command Reference</i>	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). Note For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
<i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<i>Cisco IOS VPDN Configuration Guide</i> <i>Cisco IOS XE VPDN Configuration Guide</i> <i>Cisco IOS VPDN Command Reference</i>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
<i>Cisco IOS Wide-Area Networking Configuration Guide</i> <i>Cisco IOS XE Wide-Area Networking Configuration Guide</i> <i>Cisco IOS Wide-Area Networking Command Reference</i>	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
<i>Cisco IOS Wireless LAN Configuration Guide</i> <i>Cisco IOS Wireless LAN Command Reference</i>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title	Description
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS releases.
<i>Cisco IOS New, Modified, Removed, and Replaced Commands</i>	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
<i>Cisco IOS Software System Messages</i>	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of debug commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

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.

© 2007–2008 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last updated: August 6, 2008

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xii](#)
- [Additional Information, page xii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS and Cisco IOS XE Software Documentation](#)” document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page viii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the logout or exit command.	<ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the enable command.	Router#	Issue the disable command or the exit command to return to user EXEC mode.	<ul style="list-style-type: none"> • Issue show and debug commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the configure terminal command.	Router(config)#	Issue the exit command or the end command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the interface command.	Router(config-if)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the line vty or line console command.	Router(config-line)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the reload command. Press the Break key during the first 60 seconds while the system is booting.	rommon # > The # symbol represents the line number and increments at each prompt.	Issue the continue command.	<ul style="list-style-type: none"> Run as the default operating mode when a valid image cannot be loaded. Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> A user-configured access policy was configured using the transport-map command, which directed the user into diagnostic mode. The router was accessed using an RP auxiliary port. A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered, and the router was configured to enter diagnostic mode when the break signal was received. 	Router(diag)#	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> Inspect various states on the router, including the Cisco IOS state. Replace or roll back the configuration. Provide methods of restarting the Cisco IOS software or other processes. Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



Note

A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

?

```
Router# ?
```

```
Exec commands:
```

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

```
<snip>
```

partial command?

```
Router(config)# zo?
zone zone-pair
```

partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

command?

```
Router(config-if)# pppoe ?
enable Enable pppoe
max-sessions Maximum PPPOE sessions
```

command keyword?

```
Router(config-if)# pppoe enable ?
group attach a BBA group
<cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 3](#) describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```

Router(config)# ethernet cfm domain ?
    WORD  domain name
Router(config)# ethernet cfm domain dname ?
    level
Router(config)# ethernet cfm domain dname level ?
    <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
    <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
    protocol  protocol options
    <cr>
Router(config)# logging host ?
    Hostname or A.B.C.D  IP address of the syslog server
    ipv6                  Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
    protocol  protocol options
    <cr>

```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.



Note

Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.



Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or un	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.



Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- [Cisco IOS Release 12.2SR System Message Guide](#)
- [Cisco IOS System Messages, Volume 1 of 2](#) (Cisco IOS Release 12.4)
- [Cisco IOS System Messages, Volume 2 of 2](#) (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
or
“Using Cisco IOS XE Software” chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:
http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html
- Cisco Product Support Resources
<http://www.cisco.com/web/psa/products/index.html>
- Support area on Cisco.com (also search for documentation by task or product)
<http://www.cisco.com/en/US/support/index.html>
- *White Paper: Cisco IOS Reference Guide*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

<http://tools.cisco.com/Support/CLILookup>

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

<https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

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.

© 2007–2008 Cisco Systems, Inc. All rights reserved.



Basic MPLS



Multiprotocol Label Switching Overview

This chapter describes the Multiprotocol Label Switching (MPLS) distribution protocol. MPLS is a high-performance packet forwarding technology that integrates the performance and traffic management capabilities of data link layer (Layer 2) switching with the scalability, flexibility, and performance of network-layer (Layer 3) routing. It enables service providers to meet challenges brought about by explosive growth and provides the opportunity for differentiated services without necessitating the sacrifice of existing infrastructure.

The MPLS architecture is remarkable for its flexibility:

- Data can be transferred over any combination of Layer 2 technologies
- Support is offered for all Layer 3 protocols
- Scaling is possible well beyond anything offered in today's networks.

Specifically, MPLS can efficiently enable the delivery of IP services over an ATM switched network. It supports the creation of different routes between a source and a destination on a purely router-based Internet backbone. Service providers who use MPLS can save money and increase revenue and productivity.

Procedures for configuring MPLS are provided in the [“Configuring Multiprotocol Label Switching”](#) chapter later in this publication.



Note

Label switching on a router requires that Cisco Express Forwarding (CEF) be enabled on that router. Refer to the CEF feature documentation for configuration information. For more information on enabling CEF, see the [“Configuring Cisco Express Forwarding”](#) chapter in this publication.

This chapter describes MPLS. It contains the following sections:

- [MPLS/Tag Switching Terminology](#)
- [MPLS Commands and Saved Configurations](#)
- [MPLS/Tag Switching CLI Command Summary](#)
- [Benefits](#)
- [Label Switching Functions](#)
- [Distribution of Label Bindings](#)
- [MPLS and Routing](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [MPLS Traffic Engineering](#)
- [MPLS Virtual Private Networks](#)
- [MPLS Quality of Service](#)
- [MPLS Label Switch Controller](#)
- [MPLS Egress NetFlow Accounting](#)

MPLS/Tag Switching Terminology

Beginning with Cisco IOS Release 12.1, the Tag Switching distribution protocol has been replaced with the MPLS distribution protocol. MPLS supports the following:

- Tag Switching features
- Tag Switching command-line interface (CLI) commands

[Table 22](#) lists tag switching terms (found in earlier releases of this document) and the equivalent MPLS terms used in this document.

Table 22 *Equivalency Table for Tag Switching and MPLS Terms*

Old Tag Switching Terminology	New MPLS Terminology
Tag Switching	Multiprotocol Label Switching (MPLS)
Tag (short for Tag Switching)	MPLS
Tag (item or packet)	Label
TDP (Tag Distribution Protocol)	LDP (Label Distribution Protocol) Cisco TDP and LDP (MPLS Label Distribution Protocol) are nearly identical in function, but use incompatible message formats and some different procedures. Cisco is changing from TDP to a fully compliant LDP.
Tag Switched	Label Switched
TFIB (Tag Forwarding Information Base)	LFIB (Label Forwarding Information Base)
TSR (Tag Switching Router)	LSR (Label Switching Router)
TSC (Tag Switch Controller)	LSC (Label Switch Controller)
ATM-TSR (ATM Tag Switch Router)	ATM-LSR (ATM Label Switch Router, such as the Cisco BPX 8650 switch)
TVC (Tag VC, Tag Virtual Circuit)	LVC (Label VC, Label Virtual Circuit)
TSP (Tag Switch Path)	LSP (Label Switch Path)
XTag ATM (extended Tag ATM port)	XmplsATM (extended MPLS ATM port)

MPLS Commands and Saved Configurations

During the transition period from tag switching to MPLS, if a configuration command has both MPLS and tag switching forms, the tag switching version is written to saved configurations. For example, you can configure MPLS hop-by-hop forwarding for a router POS interface by issuing the following commands:

```
Router# configure terminal
Router(config)# interface POS3/0
Router(config-if)# mpls ip
```

In this example, the **mpls ip** command has a tag switching form (**tag-switching ip**). After you enter these commands and save this configuration or display the running configuration by means of the **show running configuration** command, the configuration commands appear as follows:

```
interface POS3/0
tag-switching ip
```

Saving the tag switching form of commands (that have both tag switching and MPLS forms) allows for backward compatibility. You can use a new router software image to modify and write configurations, and then later use configurations created by the new image with earlier software versions that do not support the MPLS forms of commands.

Using the tag switching forms of the commands allows older software that supports tag switching commands, but not new MPLS commands, to successfully interpret interface configurations.

MPLS/Tag Switching CLI Command Summary

Table 23 summarizes general-purpose MPLS commands. Except where otherwise noted, these MPLS commands have been derived from existing tag-switching commands to preserve the familiar syntax of existing commands that formed the basis for implementing new MPLS functionality.

Table 23 Summary of MPLS Commands Described in this Document

Command	Corresponding Tag Switching Command	Description
debug mpls adjacency	debug tag-switching adjacency	Displays changes to label switching entries in the adjacency database.
debug mpls events	debug tag-switching events	Displays information about significant MPLS events.
debug mpls lfib cef	debug tag-switching tfib cef	Prints detailed information about label rewrites being created, resolved, and deactivated as CEF routes are added, changed, or removed.
debug mpls lfib enc	debug tag-switching tfib enc	Prints detailed information about label encapsulations while label rewrites are created or updated and placed into the label forwarding information base (LFIB).
debug mpls lfib lsp	debug tag-switching tfib tsp	Prints detailed information about label rewrites being created and deleted as TSP tunnels are added or removed.
debug mpls lfib state	debug tag-switching tfib state	Traces what happens when label switching is enabled or disabled.

Table 23 Summary of MPLS Commands Described in this Document (continued)

Command	Corresponding Tag Switching Command	Description
<code>debug mpls lfib struct</code>	<code>debug tag-switching tfib struct</code>	Traces the allocation and freeing of LFIB-related data structures, such as the LFIB itself, label-rewrites, and label-info data.
<code>debug mpls packets</code>	<code>debug tag-switching packets</code>	Displays labeled packets switched by the host router.
<code>interface atm</code>	<code>interface atm</code>	Enters interface configuration mode, specifies ATM as the interface type, and enables the creation of a subinterface on the ATM interface.
<code>mpls atm control-vc</code>	<code>tag-switching atm control-vc</code>	Configures the VPI and VCI to be used for the initial link to the label switching peer device.
<code>mpls atm vpi</code>	<code>tag-switching atm vpi</code>	Configures the range of values to be used in the VPI field for label VCs.
<code>mpls ip (global configuration)</code>	<code>tag-switching ip (global configuration)</code>	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
<code>mpls ip (interface configuration)</code>	<code>tag-switching ip (interface configuration)</code>	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.
<code>mpls ip default-route</code>	<code>tag-switching ip default-route</code>	Enables the distribution of labels associated with the IP default route.
<code>mpls ip propagate-ttl</code>	<code>tag-switching ip propagate-ttl</code>	Sets the time-to-live (TTL) value when an IP packet is encapsulated in MPLS.
<code>mpls ip ttl-expiration pop</code>	N/A	Forwards packets using the global IP routing table or the original label stack, depending on the number of labels in the packet.
<code>mpls label range</code>	<code>tag-switching tag-range downstream</code>	Configures the range of local labels available for use on packet interfaces. Note The syntax of this command differs slightly from its tag-switching counterpart.
<code>mpls mtu</code>	<code>tag-switching mtu</code>	Sets the per-interface maximum transmission unit (MTU) for labeled packets.
<code>show mpls forwarding-table</code>	<code>show tag-switching forwarding-table</code>	Displays the contents of the label forwarding information base (LFIB).
<code>show mpls interfaces</code>	<code>show tag-switching interfaces</code>	Displays information about one or more interfaces that have been configured for label switching.
<code>show mpls label range</code>	N/A	Displays the range of local labels available for use on packet interfaces.

Benefits

MPLS provides the following major benefits to service provider networks:

- Scalable support for SVirtual Private Networks (VPNs)—MPLS enables VPN services to be supported in service provider networks, thereby greatly accelerating Internet growth.

The use of MPLS for VPNs provides an attractive alternative to the building of VPNs by means of either ATM or Frame Relay permanent virtual circuits (PVCs) or various forms of tunneling to interconnect routers at customer sites.

Unlike the PVC VPN model, the MPLS VPN model is highly scalable and can accommodate increasing numbers of sites and customers. The MPLS VPN model also supports “any-to-any” communication among VPN sites without requiring a full mesh of PVCs or the backhauling (suboptimal routing) of traffic across the service provider network. For each MPLS VPN user, the network of the service provider appears to function as a private IP backbone over which the user can reach other sites within the VPN organization, but not the sites of any other VPN organization.

From a user perspective, the MPLS VPN model enables network routing to be dramatically simplified. For example, rather than needing to manage routing over a topologically complex virtual backbone composed of many PVCs, an MPLS VPN user can generally employ the backbone of the service provider as the default route in communicating with all of the other VPN sites.

- Explicit routing capabilities (also called constraint-based routing or traffic engineering)—Explicit routing employs “constraint-based routing,” in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow.

In MPLS traffic engineering, factors such as bandwidth requirements, media requirements, and the priority of one traffic flow versus another can be taken into account. These traffic engineering capabilities enable the administrator of a service provider network to perform the following tasks:

- Control traffic flow in the network
- Reduce congestion in the network
- Make best use of network resources

Thus, the network administrator can specify the amount of traffic expected to flow between various points in the network (thereby establishing a traffic matrix), while relying on the routing system to perform the following tasks:

- Calculate the best paths for network traffic
- Set up the explicit paths to carry the traffic

- Support for IP routing on ATM switches (also called IP and ATM integration)—MPLS enables an ATM switch to perform virtually all of the functions of an IP router. This capability of an ATM switch stems from the fact that the MPLS forwarding paradigm (namely, label swapping) is exactly the same as the forwarding paradigm provided by ATM switch hardware.

The key difference between a conventional ATM switch and an ATM label switch is the control software used by the latter to establish its virtual channel identifier (VCI) table entries. An ATM label switch uses IP routing protocols and the TDP to establish VCI table entries.

An ATM label switch can function as a conventional ATM switch. In this dual mode, the ATM switch resources (such as VCI space and bandwidth) are partitioned between the MPLS control plane and the ATM control plane. The MPLS control plane provides IP-based services, while the ATM control plane supports ATM-oriented functions, such as circuit emulation or PVC services.

Label Switching Functions

In conventional Layer 3 forwarding mechanisms, as a packet traverses the network, each router extracts all the information relevant to forwarding the packet from the Layer 3 header. This information is then used as an index for a routing table lookup to determine the next hop for the packet.

In the most common case, the only relevant field in the header is the destination address field, but in some cases other header fields might also be relevant. As a result, the header analysis must be done independently at each router through which the packet passes. A complicated table lookup must also be done at each router.

In label switching, the analysis of the Layer 3 header is done only once. The Layer 3 header is then mapped into a fixed length, unstructured value called a *label*.

Many different headers can map to the same label, as long as those headers always result in the same choice of next hop. In effect, a label represents a *forwarding equivalence class*—that is, a set of packets that, however different they may be, are indistinguishable by the forwarding function.

The initial choice of a label need not be based exclusively on the contents of the Layer 3 packet header; for example, forwarding decisions at subsequent hops can also be based on routing policy.

Once a label is assigned, a short label header is added at the front of the Layer 3 packet. This header is carried across the network as part of the packet. At subsequent hops through each MPLS router in the network, labels are swapped and forwarding decisions are made by means of MPLS forwarding table lookup for the label carried in the packet header. Hence, the packet header need not be reevaluated during packet transit through the network. Because the label is of fixed length and unstructured, the MPLS forwarding table lookup process is both straightforward and fast.

Distribution of Label Bindings

Each LSR in the network makes an independent, local decision as to which label value to use to represent a forwarding equivalence class. This association is known as a *label binding*. Each LSR informs its neighbors of the label bindings it has made. This awareness of label bindings by neighboring routers is facilitated by the following protocols:

- TDP—Used to support MPLS forwarding along normally routed paths
- Resource Reservation Protocol (RSVP)—Used to support MPLS traffic engineering
- Border Gateway Protocol (BGP)—Used to support MPLS VPNs

When a labeled packet is being sent from LSR A to the neighboring LSR B, the label value carried by the IP packet is the label value that LSR B assigned to represent the forwarding equivalence class of the packet. Thus, the label value changes as the IP packet traverses the network.

MPLS and Routing

A label represents a forwarding equivalence class, but it does not represent a particular path through the network. In general, the path through the network continues to be chosen by the existing Layer 3 routing algorithms such as OSPF, Enhanced IGRP, and BGP. That is, at each hop when a label is looked up, the next hop chosen is determined by the dynamic routing algorithm.

MPLS Traffic Engineering

MPLS traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what now can be achieved only by overlaying a Layer 3 network on a Layer 2 network.

Traffic engineering is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures.

MPLS traffic engineering provides an integrated approach to traffic engineering. With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

Why Use MPLS Traffic Engineering?

WAN connections are an expensive item in an ISP budget. Traffic engineering enables ISPs to route network traffic to offer the best service to their users in terms of throughput and delay. By making the service provider more efficient, traffic engineering reduces the cost of the network.

Currently, some ISPs base their services on an overlay model. In the overlay model, transmission facilities are managed by Layer 2 switching. The routers see only a fully meshed virtual topology, making most destinations appear one hop away. If you use the explicit Layer 2 transit layer, you can precisely control how traffic uses available bandwidth. However, the overlay model has numerous disadvantages. MPLS traffic engineering achieves the traffic engineering benefits of the overlay model without running a separate network, and without needing a non-scalable, full mesh of router interconnects.

How MPLS Traffic Engineering Works

MPLS traffic engineering automatically establishes and maintains LSPs across the backbone by using RSVP. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth.

Available resources are flooded by means of extensions to a link-state-based Interior Gateway Protocol (IGP).

Traffic engineering tunnels are calculated at the LSP head based on a fit between required and available resources (constraint-based routing). The IGP automatically routes the traffic onto these LSPs.

Typically, a packet crossing the MPLS traffic engineering backbone travels on a single LSP that connects the ingress point to the egress point.

MPLS traffic engineering is built on the following Cisco IOS mechanisms:

- IP tunnel interfaces—From a Layer 2 standpoint, an MPLS tunnel interface represents the head of an LSP. It is configured with a set of resource requirements, such as bandwidth and media requirements, and priority.

From a Layer 3 standpoint, an LSP tunnel interface is the head-end of a unidirectional virtual link to the tunnel destination.

- MPLS traffic engineering path calculation module—This calculation module operates at the LSP head. The module determines a path to use for an LSP. The path calculation uses a link-state database containing flooded topology and resource information.
- RSVP with traffic engineering extensions—RSVP operates at each LSP hop and is used to signal and maintain LSPs based on the calculated path.
- MPLS traffic engineering link management module—This module operates at each LSP hop, does link call admission on the RSVP signalling messages, and does bookkeeping of topology and resource information to be flooded.
- Link-state IGP (Intermediate System-to-Intermediate System (IS-IS) or OSPF—each with traffic engineering extensions)—These IGPs are used to globally flood topology and resource information from the link management module.
- Enhancements to the SPF calculation used by the link-state IGP (IS-IS or OSPF)—The IGP automatically routes traffic onto the appropriate LSP tunnel based on tunnel destination. Static routes can also be used to direct traffic onto LSP tunnels.
- Label switching forwarding—This forwarding mechanism provides routers with a Layer 2-like ability to direct traffic across multiple hops of the LSP established by RSVP signalling.

One approach to engineering a backbone is to define a mesh of tunnels from every ingress device to every egress device. The MPLS traffic engineering path calculation and signalling modules determine the path taken by the LSPs for these tunnels, subject to resource availability and the dynamic state of the network. The IGP, operating at an ingress device, determines which traffic should go to which egress device, and steers that traffic into the tunnel from ingress to egress.

A flow from an ingress device to an egress device might be so large that it cannot fit over a single link, so it cannot be carried by a single tunnel. In this case, multiple tunnels between a given ingress and egress can be configured, and the flow is load-shared among them.

For more information about MPLS, see the following Cisco documentation:

- *Cisco IOS Switching Services Configuration Guide*, “Multiprotocol Label Switching” chapter
- *Cisco IOS Switching Services Command Reference*, “Switching Commands Introduction” chapter

Mapping Traffic into Tunnels

This section describes how traffic is mapped into tunnels; that is, how conventional hop-by-hop link-state routing protocols interact with MPLS traffic engineering capabilities. In particular, this section describes how the shortest path first (SPF) algorithm, sometimes called a Dijkstra algorithm, has been enhanced so that a link-state IGP can automatically forward traffic over tunnels that MPLS traffic engineering establishes.

Link-state protocols, like integrated IS-IS or OSPF, use an SPF algorithm to compute a shortest path tree from the headend node to all nodes in the network. Routing tables are derived from this shortest path tree. The routing tables contain ordered sets of destination and first hop information. If a router does normal hop-by-hop routing, the first hop is over a physical interface attached to the router.

New traffic engineering algorithms calculate explicit routes to one or more nodes in the network. The originating router views these explicit routes as logical interfaces. In the context of this document, these explicit routes are represented by LSPs and referred to as traffic engineering tunnels (TE tunnels).

The following sections describe how link-state IGP's can use these shortcuts, and how they can install routes in the routing table that point to these TE tunnels. These tunnels use explicit routes, and the path taken by a TE tunnel is controlled by the router that is the headend of the tunnel. In the absence of errors, TE tunnels are guaranteed not to loop, but routers must agree on how to use the TE tunnels. Otherwise, traffic might loop through two or more tunnels.

Enhancement to the SPF Computation

During each step of the SPF computation, a router discovers the path to one node in the network, as follows:

- If that node is directly connected to the calculating router, the first hop information is derived from the adjacency database.
- If the node is not directly connected to the calculating router, the node inherits the first hop information from the parents of that node. Each node has one or more parents, and each node is the parent of zero or more downstream nodes.

For traffic engineering purposes, each router maintains a list of all TE tunnels that originate at this head end router. For each of those TE tunnels, the router at the tailend is known to the head end router.

During the SPF computation, the TENT (tentative) list stores paths that are possibly the best paths and the PATH list stores paths that are definitely the best paths. When it is determined that a path is the best possible path, the node is moved from TENT to PATH. PATH is thus the set of nodes for which the best path from the computing router has been found. Each PATH entry consists of ID, path cost, and forwarding direction.

The router must determine the first hop information using one of the following methods:

- Examine the list of tail-end routers directly reachable by a TE tunnel. If there is a TE tunnel to this node, use the TE tunnel as the first hop.
- If there is no TE tunnel and the node is directly connected, use the first hop information from the adjacency database.
- If the node is not directly connected and is not directly reachable by a TE tunnel, copy the first hop information from the parent nodes to the new node.

As a result of this computation, traffic to nodes that are the tail end of TE tunnels flows over the TE tunnels. Traffic to nodes that are downstream of the tail-end nodes also flows over the TE tunnels. If there is more than one TE tunnel to different intermediate nodes on the path to destination node X, traffic flows over the TE tunnel whose tail-end node is closest to node X.

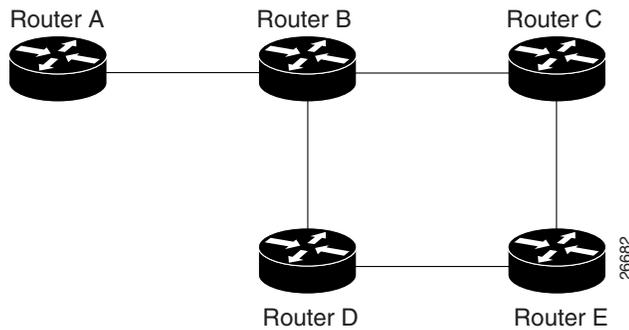
Special Cases and Exceptions

The SPF algorithm finds equal-cost parallel paths to destinations. The enhancement previously described does not change this behavior. Traffic can be forwarded over any of the following:

- One or more native IP paths
- One or more traffic engineering tunnels
- A combination of native IP paths and traffic engineering tunnels

A special situation occurs in the topology shown in [Figure 24](#).

Figure 24 *Sample Topology of Parallel Native Paths and Paths over TE Tunnels*



If parallel native IP paths and paths over TE tunnels are available, the following implementations allow you to force traffic to flow over TE tunnels only or only over native IP paths. Assume that all links have the same cost and that a TE tunnel is set up from Router A to Router D.

- When the SPF calculation puts Router C on the TENT list, it realizes that Router C is not directly connected. It uses the first hop information from the parent, which is Router B.
- When the SPF calculation on Router A puts Router D on the TENT list, it realizes that Router D is the tail end of a TE tunnel. Thus Router A installs a route to Router D by the TE tunnel, and not by Router B.
- When Router A puts Router E on the TENT list, it realizes that Router E is not directly connected, and that Router E is not the tail end of a TE tunnel. Therefore Router A copies the first hop information from the parents (Router C and Router D) to the first-hop information of Router E.

Traffic to Router E now load balances over the following:

- The native IP path by Router A to Router B to Router C
- The TE tunnel Router A to Router D

Additional Enhancements to SPF Computation Using Configured Tunnel Metrics

When traffic engineering tunnels install an IGP route in a Router Information Base (RIB) as next hops, the distance or metric of the route must be calculated. Normally, you could make the metric the same as the IGP metric over native IP paths as if the TE tunnels did not exist. For example, Router A can reach Router C with the shortest distance of 20. X is a route advertised in IGP by Router C. Route X is installed in the RIB of Router A with the metric of 20. When a TE tunnel from Router A to Router C comes up, by default the route is installed with a metric of 20, but the next hop information for X is changed.

Although the same metric scheme can work well in other situations, for some applications it is useful to change the TE tunnel metric (for instance, when there are equal cost paths through TE tunnel and native IP links). You can adjust TE tunnel metrics to force the traffic to prefer the TE tunnel, to prefer the native IP paths, or to load share among them.

Suppose that multiple TE tunnels go to the same destination or different destinations. TE tunnel metrics can force the traffic to prefer some TE tunnels over others, regardless of IGP distances to those destinations.

Setting metrics on TE tunnels does not affect the basic SPF algorithm. It affects only two questions:

- Is the TE tunnel installed as one of the next hops to the destination routers?
- What is the metric value of the routes being installed into the RIB?

You can modify the metrics for determining the first hop information in one of the following ways:

- If the metric of the TE tunnel to the tail end routers is higher than the metric for the other TE tunnels or native hop-by-hop IGP paths, this tunnel is not installed as the next hop.
- If the metric of the TE tunnel is equal to the metric of either other TE tunnels or native hop-by-hop IGP paths, this tunnel is added to the existing next hops.
- If the metric of the TE tunnel is lower than the metric of other TE tunnels or native hop-by-hop IGP paths, this tunnel replaces them as the only next hop.

In each of these cases, the IGP assigns metrics to routes associated with those tail end routers and their downstream routers.

The SPF computation is loop free because the traffic through the TE tunnels is basically source routed. The result of TE tunnel metric adjustment is the control of traffic load sharing. If there is only one way to reach the destination through a single TE tunnel, then no matter what metric is assigned, the traffic has only one way to go.

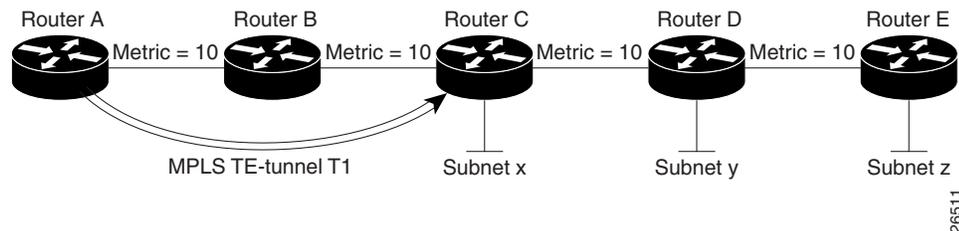
You can represent the TE tunnel metric in two different ways: as an absolute (or fixed) metric, or as a relative (or floating) metric.

If you use an absolute metric, the routes assigned with the metric are fixed. This metric is used not only for the routes sourced on the TE tunnel tail end router, but also for each route downstream of this tail end router that uses this TE tunnel as one of its next hops.

For example, if you have TE tunnels to two core routers in a remote point of presence (POP), and one of them has an absolute metric of 1, all traffic going to that POP traverses this low-metric TE tunnel.

If you use a relative metric, the actual assigned metric value of routes is based on the IGP metric. This relative metric can be positive or negative, and is bounded by minimum and maximum allowed metric values. For example, assume the topology shown in [Figure 25](#).

Figure 25 *Topology That Has No Traffic Engineering Tunnel*



If there is no TE tunnel, Router A installs routes x, y, and z and assigns metrics 20, 30, and 40, respectively. Suppose that Router A has a TE tunnel T1 to Router C. If the relative metric -5 is used on tunnel T1, the routers x, y, and z have the installed metrics of 15, 25, and 35. If an absolute metric of 5 is used on tunnel T1, routes x, y and z have the same metric 5 installed in the RIB for Router A. The assigning of no metric on the TE tunnel is a special case, a relative metric scheme where the metric is 0.

Making the Transition from an IS-IS Network to a New Technology

IS-IS includes extensions for MPLS traffic engineering and for other purposes. Running MPLS traffic engineering over IS-IS or taking advantage of these other extensions requires transition to an IS-IS network to this new technology. This section describes these extensions and discusses two ways to migrate an existing IS-IS network from the standard ISO 10589 protocol to IS-IS with new extensions.

**Note**

Running MPLS traffic engineering over an existing IS-IS network requires a transition to incorporating extensions to IS-IS. However, running MPLS traffic engineering over OSPF does *not* require any similar network transition.

New Extensions for the IS-IS Routing Protocol

New extensions for the IS-IS routing protocol serve the following purposes:

- Remove the 6-bit limit on link metrics.
- Allow interarea IP routes.
- Enable IS-IS to carry different kinds of information for traffic engineering. In the future, more extensions might be needed.

To serve these purposes, two new type, length, and value objects (TLVs) have been defined:

- TLV 22 describes links (or rather adjacencies). It serves the same purpose as the IS neighbor option in ISO 10589 (TLV 2).
- TLV 135 describes reachable IP prefixes. It is similar to the IP Neighbor options from RFC 1195 (TLVs 128 and 130).

**Note**

For the purpose of brevity, these two new TLVs, 22 and 135, are referred to as “new-style TLVs.” TLVs 2, 128, and 130 are referred to as “old-style TLVs.”

Both new TLVs have a fixed length part, followed by optional sub-TLVs. The metric space in these new TLVs has been enhanced from 6 bits to 24 or 32 bits. The sub-TLVs allow you to add new properties to links and prefixes. Traffic engineering is the first technology to use this ability to add new properties to a link.

The Problem in Theory

Link-state routing protocols compute loop-free routes. This is guaranteed because all routers calculate their routing tables based on the same information from the link-state database.

There is a problem when some routers look at old-style TLVs and some routers look at new-style TLVs because the routers can base their SPF calculations on different information. This can cause routing loops.

The Problem in Practice

The easiest way to migrate from old-style TLVs to new-style TLVs would be to introduce a “flag day.” A flag day means that you reconfigure all routers during a short period of time, during which service is interrupted. If the implementation of a flag day is not acceptable, a network administrator needs to find a viable solution for modern existing networks.

Network administrators have the following problems related to TLVs:

- They need to run an IS-IS network where some routers are advertising and using the new-style TLVs and, at the same time, other routers are capable only of advertising and using old-style TLVs.

- They need to test new traffic engineering software in existing networks on a limited number of routers. They cannot upgrade all their routers in their production networks or in their test networks before they start testing.

The new extensions allow a network administrator to use old-style TLVs in one area, and new-style TLVs in another area. However, this is not a solution for administrators that need or want to run their network in one single area.

The following sections describe two solutions to the problem of the network administrator.

First Solution for Making the Transition from an IS-IS Network to a New Technology

When you migrate from old-style TLVs to new-style TLVs, you can advertise the same information twice—once in old-style TLVs and once in new-style TLVs. This ensures that all routers can understand what is advertised.

There are three disadvantages to using that approach:

- Size of the LSPs—During the transition, the LSPs grow to about twice their original size. This might be a problem in networks where the link-state database is large. A link-state database might be large for the following reasons:
 - There are many routers, and thus LSPs.
 - There are many neighbors or IP prefixes per router. A router that advertises substantial information causes the LSPs to be fragmented.
- Unpredictable results—In a large network, this solution can produce unpredictable results. A large network in transition pushes the limits regarding LSP flooding and SPF scaling. During the transition, the following behavior might occur:
 - You can expect some extra network instability.
 - Traffic engineering extensions might cause LSPs to be reflooded frequently.
- Ambiguity—If a router encounters different information in the old-style TLVs and the new-style TLVs, it may not be clear what the router should do.

These problems can be largely solved easily by using the following:

- All information in old-style and new-style TLVs in an LSP
- The adjacency with the lowest link metric if an adjacency is advertised more than once

The main benefit to advertising the same information twice is that network administrators can use new-style TLVs before all routers in the network can understand them.

Transition Actions During the First Solution

When making the transition from using IS-IS with old-style TLVs to new-style TLVs, you can perform the following actions:

- If all routers run old software, advertise and use only old-style TLVs.
- Upgrade some routers to newer software.
- Configure some routers with new software to advertise both old-style and new-style TLVs. They accept both styles of TLVs. Configure other routers (with old software) to continue advertising and using only old-style TLVs.
- Test traffic engineering in parts of your network; however, new-style TLVs cannot be used yet.
- If the whole network needs to migrate, upgrade and configure all remaining routers to advertise and accept both styles of TLVs.

- Configure all routers to advertise and accept only new-style TLVs.
- Configure metrics larger than 63.

For more information about how to perform these actions, see the section “[TLV Configuration Commands](#).”

Second Solution for Making the Transition from an IS-IS Network to a New Technology

Routers advertise only one style of TLVs at the same time, but can understand both types of TLVs during migration. There are two main benefits to this approach:

- LSPs stay approximately the same size during migration.
- There is no ambiguity when the same information is advertised twice inside one LSP.

This method is useful when you move the whole network (or a whole area) to use wider metrics (that is, you want a router running IS-IS to generate and accept only new-style TLVs). For more information, see the **metric-style wide** router configuration command.

The disadvantage is that all routers must understand the new-style TLVs before any router can start advertising new-style TLVs. It does not help the second problem, where network administrators want to use the new-style TLVs for traffic engineering, while some routers are capable of understanding only old-style TLVs.

Transition Actions During the Second Solution

If you use the second solution, you can perform the following actions:

- If all routers run old software, advertise and use only old-style TLVs.
- Upgrade all routers to newer software.
- Configure all routers one-by-one to advertise old-style TLVs, but to accept both styles of TLVs.
- Configure all routers one-by-one to advertise new-style TLVs, but to accept both styles of TLVs.
- Configure all routers one-by-one to advertise and to accept only new-style TLVs.
- Configure metrics larger than 63.

TLV Configuration Commands

Cisco IOS software has a new router isis CLI command called **metric-style**. Once you are in the router IS-IS command mode, you have the option to choose the following:

- **Metric-style narrow**—Enables the router to generate and accept only old-style TLVs
- **Metric-style transition**—Enables the router to generate and accept both old-style and new-style TLVs
- **Metric-style wide**—Enables the router to generate and accept only new-style TLVs

You can use either of two transition schemes when you are using the metric-style commands:

- Narrow to transition to wide
- Narrow to narrow transition to wide transition to wide

Implementation in Cisco IOS Software

Cisco IOS software implements both transition solutions of moving your IS-IS network to a new technology. Network administrators can choose the solution that suits them. For test networks, the first solution is ideal (see the section [“First Solution for Making the Transition from an IS-IS Network to a New Technology”](#)). For a real transition, both solutions can be used. The first solution requires fewer steps and less configuration. Only the largest networks that do not want to double their link-state database during transition need to use the second solution (see the [“Second Solution for Making the Transition from an IS-IS Network to a New Technology”](#)).

MPLS Virtual Private Networks

Using MPLS VPNs in a Cisco IOS network provide the capability to deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services to business customers. A VPN is a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

A one-to-one relationship does not necessarily exist between customer sites and VPNs; a given site can be a member of multiple VPNs. However, a site can associate with only one VPN routing and forwarding instance (VRF). Each VPN is associated with one or more VPN VRFs. A VRF includes routing and forwarding tables and rules that define the VPN membership of customer devices attached to CE routers. A VRF consists of the following:

- IP routing table
- CEF table
- Set of interfaces that use the CEF forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VPN routing information is stored in the IP routing table and the CEF table for each VRF. A separate set of routing and CEF tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN and also prevent packets that are outside a VPN from being forwarded to a router within the VPN.

The following sections provide more information on MPLS VPNs:

- [Benefits](#)
- [VPN Operation](#)
- [Distribution of VPN Routing Information](#)
- [BGP Distribution of VPN Routing Information](#)
- [MPLS Forwarding](#)
- [MPLS VPN Cable Interfaces](#)
- [Interautonomous Systems for MPLS VPNs](#)
- [HSRP Support for MPLS VPNS](#)

Benefits

MPLS VPNs allow service providers to deploy scalable VPNs and build the foundation to deliver value-added services, including the following:

- **Connectionless service**—A significant technical advantage of MPLS VPNs is that they are connectionless. The Internet owes its success to its basic technology, TCP/IP. TCP/IP is built on packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate. To establish privacy in a connectionless IP environment, current VPN solutions impose a connection-oriented, point-to-point overlay on the network. Even if it runs over a connectionless network, a VPN cannot take advantage of the ease of connectivity and multiple services available in connectionless networks. When you create a connectionless VPN, you do not need tunnels and encryption for network privacy, thus eliminating substantial complexity.
- **Centralized service**—Building VPNs in Layer 3 allows delivery of targeted services to a group of users represented by a VPN. A VPN must give service providers more than a mechanism for privately connecting users to intranet services. It must also provide a way to flexibly deliver value-added services to targeted customers. Scalability is critical, because customers want to use services privately in their intranets and extranets. Because MPLS VPNs are seen as private intranets, you may use IP services such as the following:
 - Multicast
 - Quality of service (QoS)
 - Telephony support within a VPN
 - Centralized services including content and web hosting to a VPN

You can customize several combinations of specialized services for individual customers. For example, a service that combines IP multicast with a low-latency service class enables videoconferencing within an intranet.

- **Scalability**—If you create a VPN using connection-oriented, point-to-point overlays, Frame Relay, or ATM virtual connections, the VPN's key deficiency of the VPN is scalability. Specifically, connection-oriented VPNs without fully meshed connections between customer sites are not optimal. MPLS-based VPNs instead use the peer model and Layer 3 connectionless architecture to leverage a highly scalable VPN solution. The peer model requires a customer site to only peer with one provider edge (PE) router as opposed to all other CPE or CE routers that are members of the VPN. The connectionless architecture allows the creation of VPNs in Layer 3, eliminating the need for tunnels or virtual connections.

The following are scalability issues of MPLS VPNs due to the partitioning of VPN routes between PE routers and the further partitioning of VPN and IGP routes between PE routers and provider (P) routers in a core network:

- PE routers must maintain VPN routes for those VPNs that are members.
- P routers do not maintain any VPN routes.

This increases the scalability of the provider's core and ensures that no one device is a scalability bottleneck.

- **Security**—MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN. Security is provided
 - At the edge of a provider network, ensuring that packets received from a customer are placed on the correct VPN.

- At the backbone, ensuring that VPN traffic is kept separate. Malicious spoofing (an attempt to gain access to a PE router) is nearly impossible because the packets received from customers are IP packets. These IP packets must be received on a particular interface or subinterface to be uniquely identified with a VPN label.
- Easy to create—To take full advantage of VPNs, it must be easy for you to create new VPNs and user communities. Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required. You can add sites to intranets and extranets and form closed user groups. When you manage VPNs in this manner, it enables membership of any given site in multiple VPNs, maximizing flexibility in building intranets and extranets.
- Flexible addressing—To make a VPN service more accessible, customers of a service provider can design their own addressing plan, independent of addressing plans for other service provider customers. Many customers use private address spaces and do not want to invest the time and expense of converting to public IP addresses to enable intranet connectivity. MPLS VPNs allow customers to continue to use their present address spaces without Network Address Translation (NAT) by providing a public and private view of the address. A NAT is required only if two VPNs with overlapping address spaces want to communicate. This enables customers to use their own unregistered private addresses, and to communicate freely across a public IP network.
- Integrated Quality of Service (QoS) support—QoS is an important requirement for many IP VPN customers. It provides the ability to address two fundamental VPN requirements:
 - Predictable performance and policy implementation
 - Support for multiple levels of service in an MPLS VPN

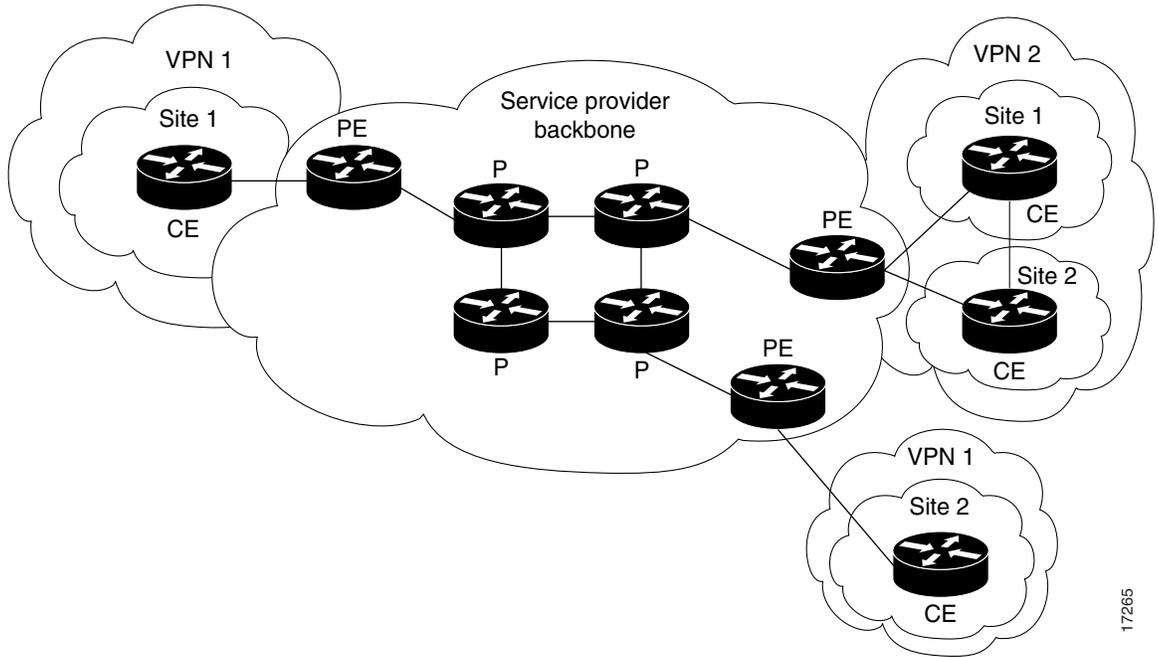
Network traffic is classified and labeled at the edge of the network before traffic is aggregated according to policies defined by subscribers and implemented by the provider and transported across the provider core. Traffic at the edge and core of the network can then be differentiated into different classes by drop probability or delay.

- Straightforward migration—For service providers to quickly deploy VPN services, use a straightforward migration path. MPLS VPNs are unique because you can build them over multiple network architectures, including IP, ATM, Frame Relay, and hybrid networks.

Migration for the end customer is simplified because there is no requirement to support MPLS on the CE router and no modifications are required to a intranet belonging to a customer.

[Figure 26](#) shows an example of a VPN with a service provider (P) backbone network, service provider edge routers (PE), and customer edge routers (CE).

Figure 26 *VPNs with a Service Provider Backbone*



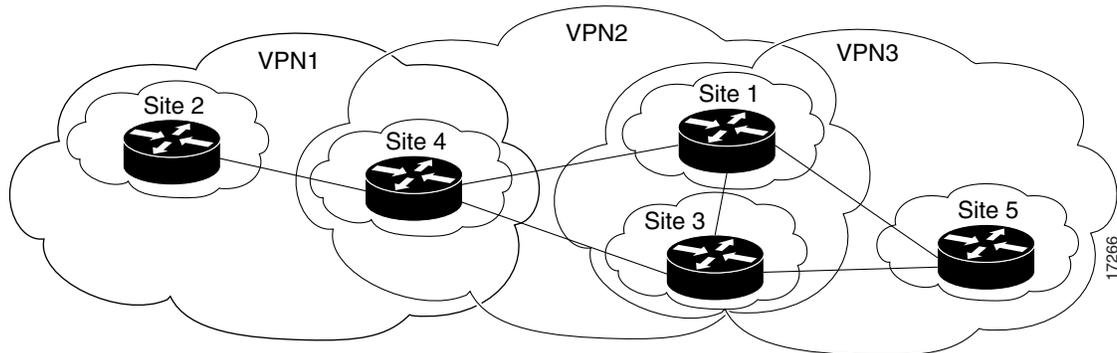
17265

A VPN contains customer devices attached to the CE routers. These customer devices use VPNs to exchange information between devices. Only the PE routers are aware of the VPNs.

Figure 27 shows five customer sites communicating within three VPNs. The VPNs can communicate with the following sites:

- VPN1—Sites 2 and 4
- VPN2—Sites 1, 3, and 4
- VPN3—Sites 1,3, and 5

Figure 27 *Customer Sites within VPNs*



17266

Increased BGP Functionality

The following is a list of increased BGP functionality:

- Configuring BGP hub and spoke connections—Configuring PE routers in a hub and spoke configuration allows a CE router to readvertise all prefixes containing duplicate autonomous system numbers (ASNs) to neighboring PE routers. Using duplicate ASNs in a hub and spoke configuration provides faster convergence of routing information within geographically dispersed locations.
- Configuring faster convergence for BGP VRF routes—Configuring scanning intervals of BGP routers decreases import processing time of VPNv4 routing information, thereby providing faster convergence of routing information. Routing tables are updated with routing information about VPNv4 routes learned from PE routers or route reflectors.
- Limiting VPN VRFs—Limiting the number of routes in a VRF prevents a PE router from importing too many routes, thus diminishing the performance of a router. This enhancement can also be used to enforce the maximum number of members that can join a VPN from a particular site. A threshold is set in the VRF routing table to limit the number of VRF routes imported.
- Reusing ASNs in an MPLS VPN environment—Configuring a PE router to reuse an existing ASN allows customers to configure BGP routes with the same ASNs in multiple geographically dispersed sites, providing better scalability between sites.
- Distributing BGP OSPF routing information—Setting a separate router ID for each interface or subinterface on a PE router attached to multiple CE routers within a VPN provides increased flexibility through OSPF when routers exchange routing information between sites.

Table 24 lists the MPLS VPN features and the associated BGP commands.

Table 24 *MPLS VPN Features and the Associated BGP Commands*

Name of Cisco IOS Feature	Command	Description
Configuring Faster Convergence for BGP VRF Routes	bgp scan-time import	Configures scanning intervals of BGP routers to decrease import processing time of routing information.
Limiting VRF Routes	maximum routes	Limits the number of routes in a VRF to prevent a PE router from importing too many routes.
Configuring BGP Hub and Spoke Connections	neighbor allowas-in	Configures PE routers to allow CE routers to readvertise all prefixes that contain duplicate ASNs to neighboring PE routers.
Reusing ASNs in an MPLS VPN Environment	neighbor as-override	Configures a PE router to reuse the same ASN on all sites within an MPLS VPN by overriding private ASNs.
Distributing BGP OSPF Routing Information	set ospf router-id	Sets a separate router ID for each interface or subinterface on the PE router for each directly attached CE router.

VPN Operation

Each VPN is associated with one or more VRFs. A VRF defines the VPN membership of a customer site attached to a PE router. A VRF consists of an IP routing table, a derived CEF table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included into the routing table.

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs, as shown in [Figure 27](#). However, a site can only associate with one (and only one) VRF. A customer's site VRF contains all the routes available to the site from the VPNs of which it is a member.

Packet forwarding information is stored in the IP routing table and the CEF table for each VRF. A separate set of routing and CEF tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN, and also prevent packets that are outside a VPN from being forwarded to a router within the VPN.

Distribution of VPN Routing Information

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. Distribution of VPN routing information works as follows:

- When a VPN route learned from a CE router is injected into BGP, a list of VPN route target extended community attributes is associated with it. Typically the list of route target community extended values is set from an export list of route targets associated with the VRF from which the route was learned.
- An import list of route target extended communities is associated with each VRF. The import list defines route target extended community attributes that a route must have in order for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target extended communities A, B, and C, then any VPN route that carries any of those route target extended communities—A, B, or C—is imported into the VRF.

BGP Distribution of VPN Routing Information

A PE router can learn an IP prefix from a CE router by static configuration, through a BGP session with the CE router, or through the Routing Information Protocol (RIP) exchange with the CE router. The IP prefix is a member of the IPv4 address family. After it learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses.

The RD used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the VRF on the PE router.

BGP distributes reachability information for VPN-IPv4 prefixes for each VPN. BGP communication takes place at two levels: within IP domains, known as autonomous systems (Interior BGP or IBGP) and between autonomous systems (Exterior BGP or EBGP). PE-PE or PE-RR (route reflector) sessions are IBGP sessions, and PE-CE sessions are EBGP sessions.

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions, which define support for address families other than IPv4. It does this in a way that ensures that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate.

MPLS Forwarding

Based on routing information stored in the VRF IP routing table and VRF CEF table, packets are forwarded to their destination using MPLS.

A PE router binds a label to each customer prefix learned from a CE router and includes the label in the network-layer reachability information (NLRI) for the prefix that it advertises to other PE routers. When a PE router forwards a packet received from a CE router across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet, it pops the label and uses it to direct the packet to the correct CE router. Label forwarding across the provider backbone, is based on either dynamic label switching or traffic engineered paths. A customer data packet carries two levels of labels when traversing the backbone:

- The top label directs the packet to the correct PE router.
- The second label indicates how that PE router should forward the packet to the CE router.

MPLS VPN Cable Interfaces

Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared hybrid fiber coaxial (HFC) network and IP infrastructure.

The cable MPLS VPN network consists of the following:

- The multiple service operator (MSO) or cable company that owns the physical infrastructure and builds VPNs for the 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.

Each ISP moves traffic to and from the PC of a subscriber, through the physical network infrastructure of the MSO, to the network of the ISP. MPLS VPNs, created in Layer 3, provide privacy and security by constraining the distribution of the routes of a VPN only to the routers that belong to its network. Thus, each VPN of the ISP is insulated from other ISPs that use the same MSO infrastructure.

An MPLS VPN assigns a unique 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. It looks up a IP destination address of a packet in the appropriate VRF table, only if the packet arrived directly through an interface associated with that table.

MPLS VPNs use a combination of BGP and IP address resolution to ensure security. Refer to the “Configuring Multiprotocol Label Switching” chapter later in this publication.

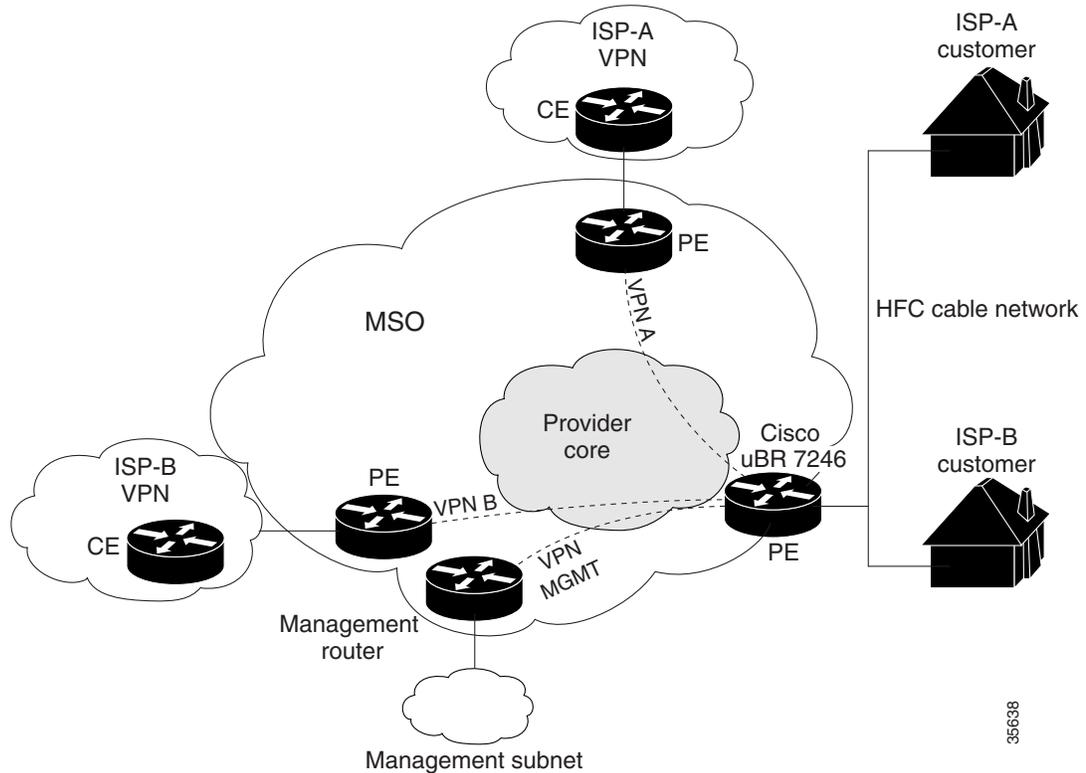
Figure 28 shows a cable MPLS VPN network. The routers in the network are as follows:

- Provider (P) router—Routers in the core of the provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS label in each route assigned by the PE router) to routed packets. VPN labels are used to direct data packets to the correct egress router.
- PE router—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 uBR7200 series router acts as a PE router.
- Customer (C) router—Router in the ISP or enterprise network.
- Customer Edge (CE) router—Edge router on the network of the ISP that connects to the PE router on the network of the MSO. A CE router must interface with a PE router.

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 Cisco uBR7200 series router to a PE router, which connects to management servers such as Cisco Network Registrar (CNR) and Time of Day (ToD) servers. A PE router connects to management

servers and is a part of the management VPN. Regardless of the ISP they belong to, the management servers serve the Dynamic Host Configuration Protocol (DHCP), DNS (Domain Name System), and ToD requests coming from PCs or cable modems.

Figure 28 *MPLS VPN Network*



Cable VPN configuration involves the following:

- 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, CM host names, routing modifications, privilege levels, and usernames and passwords.
- 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

We recommend 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.

In an MPLS VPN configuration, the MSO must configure the following:

- CMTS (Cisco uBR7200 series routers)
- P routers
- PE routers
- CE routers

- One VPN per ISP DOCSIS server for all cable modem customers. The MSO must attach DOCSIS servers to the management VPN, and make them visible.

The MSO must configure Cisco uBR7200 series routers that serve the ISP, and remote PE routers connecting to the ISP, as PE routers in the VPN.

The MSO must determine the primary IP address range, which is the range of the MSO for all cable modems belonging to the ISP subscribers.

The ISP must determine the secondary IP address range, which is the range of the ISP 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** cable interface command in Cisco IOS software. The MSO can specify the host IP address to be accessible only in the VPN of the ISP. This lets the ISP use its DHCP server to allocate IP addresses. Cable modem IP addresses must be accessible from the management VPN.

The MPLS VPN approach of creating VPNs for individual ISPs or customers requires subinterfaces to be configured on the cable interface or the cable interface bundle. Each ISP requires one subinterface. The subinterfaces are tied to the VRF tables for their respective ISPs. The first subinterface must be created on the cable interface bound to the management VPN.

To route a reply from the CNR back to the cable modem, the PE router that connects to the CNR must import the routes of the ISP VPN into the management VPN. Similarly, to forward management requests (such as DHCP renewal to CNR) to the cable modems, the ISP VPN must export and import the appropriate management VPN routes.

Cisco uBR7200 series software supports the definition of logical network-layer interfaces over a physical cable interface or a bundle of cable interfaces. You can create subinterfaces on either a physical cable interface or a bundle of cable interfaces. Subinterfaces let service providers share one IP subnet across multiple cable interfaces grouped into a cable interface bundle.

You can group all of the cable interfaces on a Cisco uBR7200 series router into a single bundle so that only one subnet is required for each router. When you group cable interfaces, no separate IP subnet or each individual cable interface is required. This grouping avoids performance, memory, and security problems in using a bridging solution to manage subnets, especially for a large number of subscribers.

Subinterfaces allow traffic to be differentiated on a single physical interface, and assigned to multiple VPNs. You can configure multiple subinterfaces, and associate an MPLS VPN with each subinterface. You can split a single physical interface (the cable plant) into multiple subinterfaces, where each subinterface is associated with a specific VPN. Each ISP requires access on a physical interface and is given its own subinterface. Create a management subinterface to support cable modem initialization from an ISP.

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. When properly configured, subscriber traffic enters the appropriate subinterface and VPN.

The CMTS MSO administrator can define subinterfaces on a cable physical interface and assign Layer 3 configurations to each subinterface, or bundle a group of physical interfaces, define subinterfaces on the bundle master, and give each subinterface a Layer 3 configuration.

Benefits

MPLS VPNs with cable interfaces provide 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 PC of a subscriber through a physical cable plant of a MSO 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 own network of a MSO using VPN technology.
- Subscribers can select combinations of services from various service providers.
- The Cisco IOS MPLS VPN cable feature sets build on CMTS DOCSIS 1.0 and DOCSIS 1.0 extensions to ensure that services are reliably and optimally delivered over the cable plant. MPLS VPN provides systems support domain selection, authentication per subscriber, selection of Quality of Service (QoS), policy-based routing (PBR), and the 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.
- Cable interface bundling eliminates the need for an IP subnet on each cable interface. Instead, an IP subnet is only required for each cable interface bundle. All cable interfaces in a Cisco uBR7200 series router can be added to a single bundle.

Interautonomous Systems for MPLS VPNs

The interautonomous system for MPLS VPNs feature allows an MPLS VPN to span service providers and autonomous systems.

As VPNs grow, their requirements expand. In some cases, VPNs need to reside on different autonomous systems in different geographic areas. (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.) 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 interautonomous systems for MPLS VPNs feature provides 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 border edge routers of autonomous systems use the EBGp to exchange that information. Then, an IGP 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 IGP.
- Between autonomous systems, routing information is shared using an EBGp. An EBGp allows a service provider to set up an interdomain routing system that guarantees the loop-free exchange of routing information between separate autonomous systems.

An MPLS VPN with interautonomous 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 an 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.

Interautonomous system configurations supported in an MPLS VPN can include the following:

- **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 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.

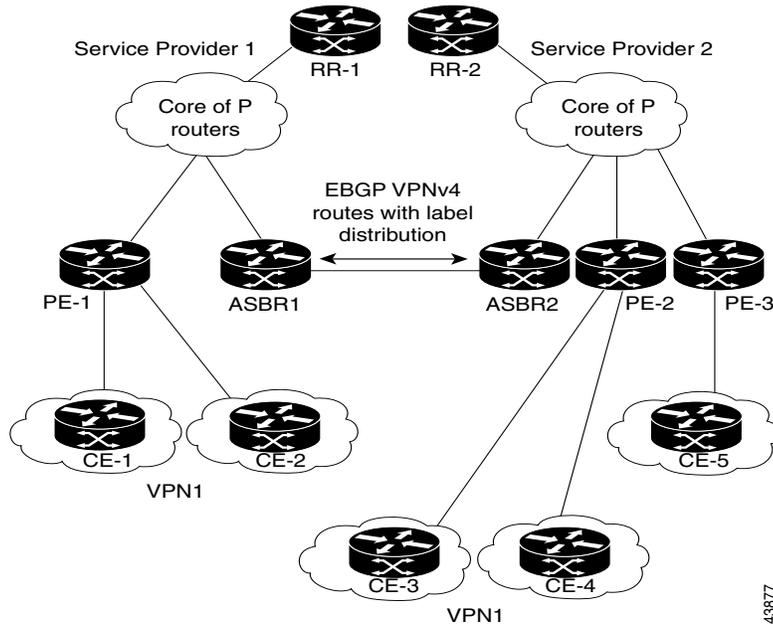
Benefits of interautonomous Systems for MPLS VPNs are as follows:

- Allows a VPN to cross more than one service provider backbone—The interautonomous 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. Previous MPLS VPNs could only traverse a single BGP autonomous system service provider backbone. The interautonomous system feature allows multiple autonomous systems to form a continuous (and seamless) network between customer sites of a service provider.
- Allows a VPN to exist in different areas—The interautonomous 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 interautonomous systems for MPLS VPNs 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 NLRI between the subautonomous systems that form the confederation.

Routing Between Autonomous Systems

Figure 29 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 29 *EBGP Connection Between Two Autonomous Systems*



This configuration uses the following process to transmit information:

-
- Step 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 BGP to send 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.
- Step 2** The two route reflectors (RR-1 and RR-2) reflect VPN-IPv4 internal routes within the autonomous system. The border edge routers of autonomous systems (ASBR1 and ASBR2) advertise the VPN-IPv4 external routes.
- Step 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 address ensures the following:
- That the next hop router is always reachable in the service provider (P) backbone network.
 - That 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.)
- Step 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** router configuration command, ASBR2 changes the next hop address of updates received from the EBGP peer, then forwards it.
 - If the IBGP neighbors are not configured with the **neighbor next-hop-self** router configuration 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 an 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 30 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 (the route target value) is part of a destination network address to make the VPN-IPv4 route globally unique in the VPN service provider environment.
- When a router redistributes the route, it reassigns the label value and sets the next hop field to the address of the distributing router (next-hop-self). Each VPN-IPv4 NRLI includes an MPLS label. When a router changes the next hop field for a route, it changes the label field to a value that is significant to the next hop destination router.

Figure 30 Exchanging Routes and Labels Between Autonomous Systems in an Interprovider VPN Network

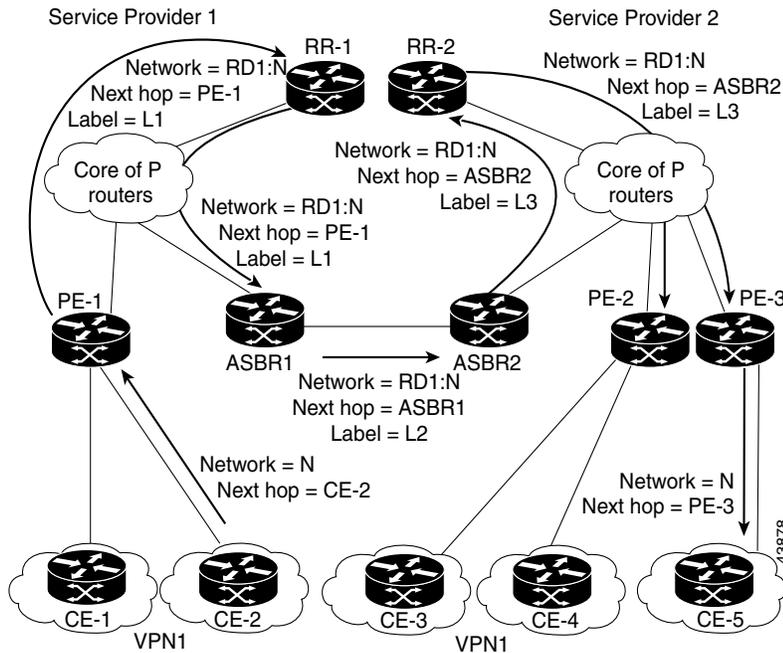
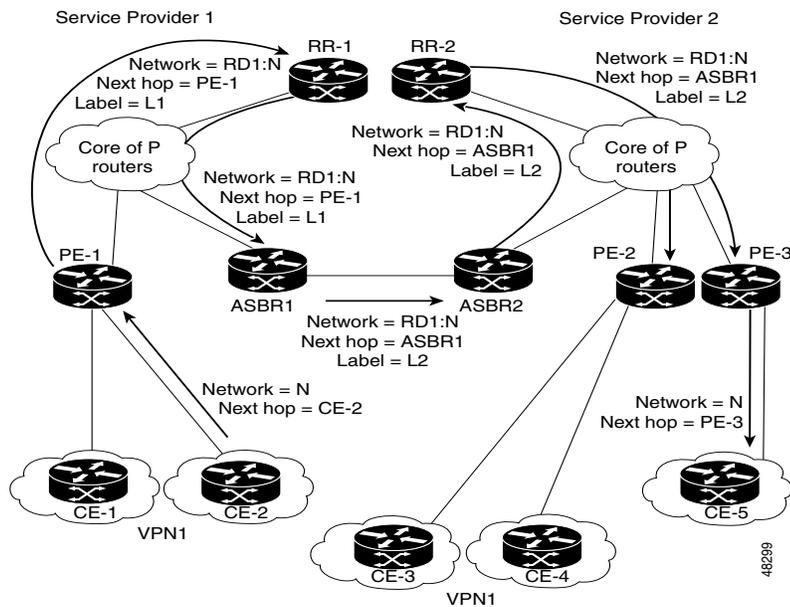


Figure 31 illustrates the exchange of VPN route and label information between autonomous systems. The difference between Figure 30 and Figure 31 is that ASBR2 is configured with the **redistribute connected** router configuration command, which propagates the host routes to all PEs. The **redistribute connected** router configuration command is necessary because ASBR2 is not configured to change the next hop address.

Figure 31 Exchanging Routes and Labels Between Autonomous Systems in an Interprovider VPN Network



Packet Forwarding

Figure 32 illustrates how packets are forwarded between autonomous systems in an interprovider network using the following packet forwarding method.

Packets are forwarded to their destination by means of 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 multilevel 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 32 Forwarding Packets Between Autonomous Systems in an Interprovider VPN Network

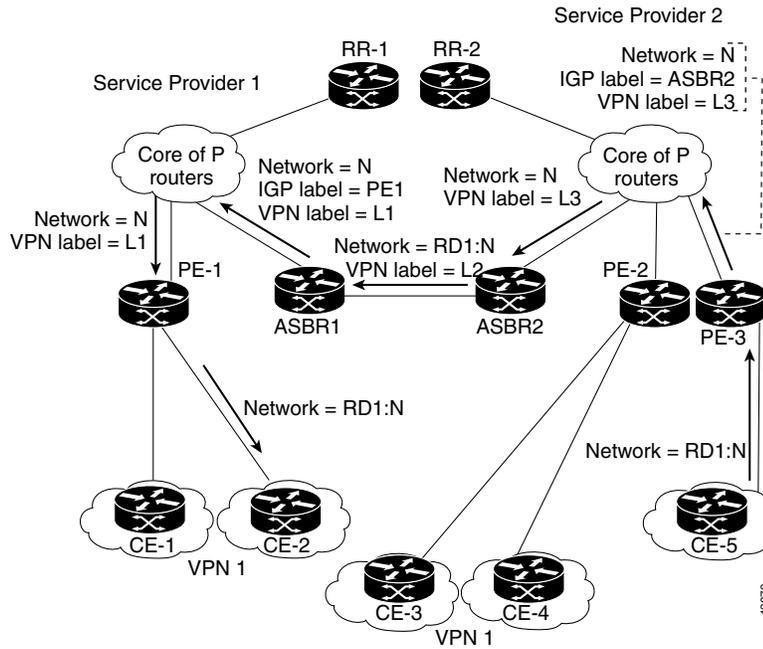
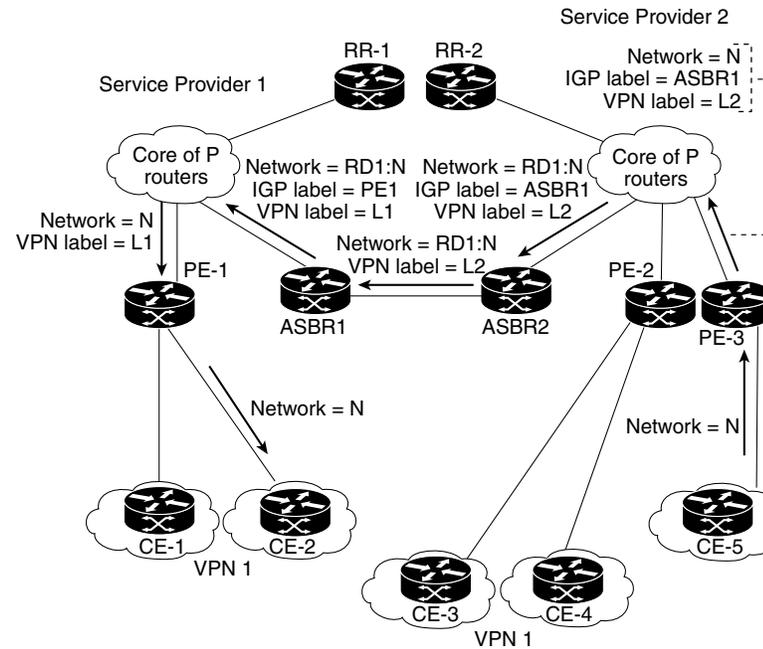


Figure 33 illustrates the same packet forwarding method, except the EBGP router (ASBR1) forwards the packet without reassigning it a new label.

Figure 33 Forwarding Packets Between Autonomous Systems in an Interprovider VPN Network



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 OSPF or 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:

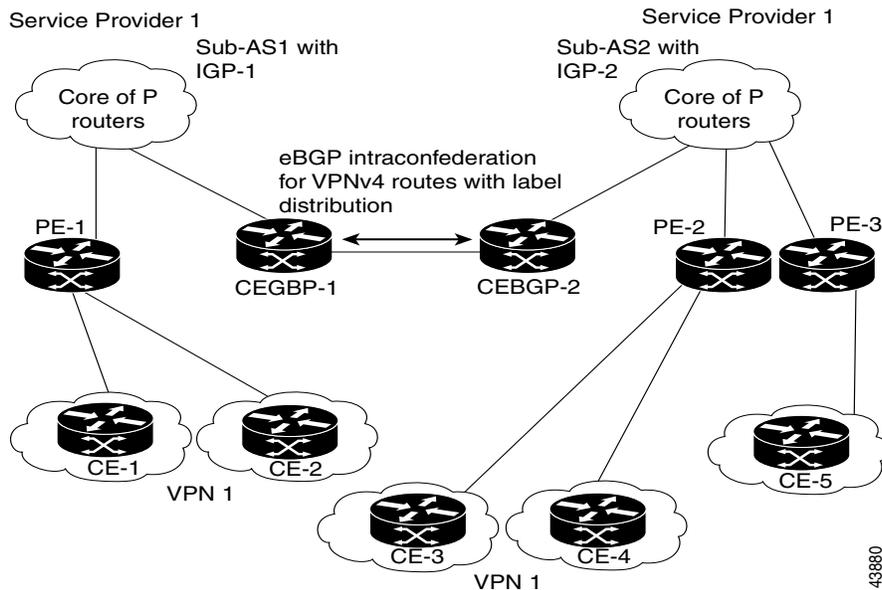
- You can configure a router to forward next-hop-self addresses between only the CEBGP border edge routers (both directions). The subautonomous systems (IBGP peers) at the subautonomous system border do not forward the next-hop-self address. Each subautonomous system runs as a single IGP domain. However, 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.

**Note**

[Figure 30](#) and [Figure 31](#) illustrate how two autonomous systems exchange routes and forward packets. Subautonomous systems in a confederation use a similar method of exchanging routes and forwarding packets.

[Figure 34](#) illustrates a typical MPLS VPN confederation configuration. The following behavior occurs 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 34 *EBGP Connection Between Two Subautonomous Systems in a Confederation*

The following behavior occurs 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 and 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 an 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.

HSRP Support for MPLS VPNS

Hot Standby Router Protocol (HSRP) can now provide transparent “first-hop IP routing” redundancy for workstations or routers connected to interfaces within MPLS VPNS. For more information on enabling HSRP or configuring HSRP group attributes, refer to the “Configuring IP Services” chapter in the *Cisco IOS IP Configuration Guide*.

MPLS Quality of Service

The quality of service (QoS) feature for MPLS enables network administrators to provide differentiated types of service across an MPLS network. Differentiated service satisfies a range of requirements by supplying for each packet transmitted the particular kind of service specified for that packet by its QoS. Service can be specified in different ways, for example, using the IP precedence bit settings in IP packets.

In supplying differentiated service, MPLS QoS offers packet classification, congestion avoidance, and congestion management. [Table 25](#) lists these functions and their descriptions.

Table 25 QoS Services and Features

Service	QoS Function	Description
Packet classification	Committed access rate (CAR). Packets are classified at the edge of the network before labels are assigned.	Classifies packets according to input or output transmission rates. Allows you to set the MPLS experimental bits or the IP Precedence or DSCP bits (whichever is appropriate).
Congestion avoidance	Weighted Random Early Detection (WRED). Packet classes are differentiated based on drop probability.	Monitors network traffic to prevent congestion by dropping packets based on the IP Precedence or DSCP bits or the MPLS experimental field.
Congestion management	Class-based weighted fair queueing (CBWFQ). Packet classes are differentiated based on bandwidth and bounded delay.	An automated scheduling system that uses a queueing algorithm to ensure bandwidth allocation to different classes of network traffic.



Note

MPLS QoS lets you duplicate Cisco IOS IP QoS (Layer 3) features as closely as possible in MPLS devices, including label edge routers (LERs), LSRs, and ATM-LSRs. MPLS QoS functions map nearly one-for-one to IP QoS functions on all interface types.

For more information on configuration of the QoS functions (CAR, WRED, and CBWFQ), refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

For complete command syntax information for CAR, WRED, and WFQ, refer to the *Cisco IOS Quality of Service Solutions Command Reference*.

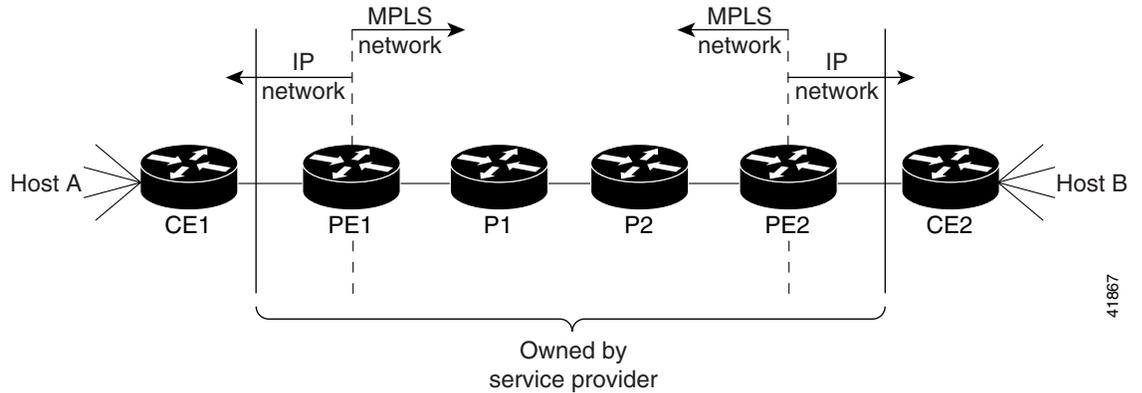
Specifying the QoS in the IP Precedence Field

When you send IP packets from one site to another, the IP Precedence field (the first three bits of the DSCP field in the header of an IP packet) specifies the QoS. Based on the IP precedence marking, the packet is given the desired treatment such as the latency or the percent of bandwidth allowed for that quality of service. If the service provider network is an MPLS network, then the IP precedence bits are copied into the MPLS EXP field at the edge of the network. However, the service provider might want to set a QoS for a MPLS packet to a different value determined by the service offering.

This feature allows the service provider to set the MPLS experimental field instead of overwriting the value in the IP precedence field belonging to a customer. The IP header remains available for the customer's use; the QoS of an IP packet is not changed as the packet travels through the MPLS network.

[Figure 35](#) shows an MPLS network that connects two sites of a IP network belonging to a customer.

Figure 35 MPLS Network Connecting Two Sites of a IP Network Belonging to a Customer



41867



Note

The network is bidirectional, but for the purpose of this document the packets move left to right.

In [Figure 35](#), the symbols have the following meanings displayed in [Table 26](#):

Table 26 Device Symbols

Symbol	Meaning
CE1	Customer equipment 1
PE1	Service provider edge router (ingress LSR)
P1	Service provider router within the core of the network of the service provider
P2	Service provider router within the core of the network of the service provider
PE2	Service provider edge router (egress LSR)
CE2	Customer equipment 2



Note

Notice that PE1 and PE2 are at the boundaries between the MPLS network and the IP network.

In [Figure 35](#), the following behavior occurs:

- Packets arrive as IP packets at PE1, the provider edge router (also known as the ingress label switching router).
- PE1 sends the packets as MPLS packets.
- Within the service provider network, there is *no IP Precedence field* for the queuing mechanism to look at because the packets are MPLS packets. The packets remain MPLS packets until they arrive at PE2, the provider edge router.
- PE2 removes the label from each packet and forwards the packets as IP packets.

This MPLS QoS enhancement allows service providers to classify packets according to their type, input interface, and other factors by setting (marking) each packet within the MPLS experimental field without changing the IP Precedence or DSCP field. For example, service providers can classify packets with or without considering the rate of the packets that PE1 receives. If the rate is a consideration, the service provider marks in-rate packets differently from out-of-rate packets.

**Note**

The MPLS experimental bits allow you to specify the QoS for an MPLS packet. The IP Precedence/DSCP bits allow you to specify the QoS for an IP packet.

MPLS Label Switch Controller

The MPLS LSC, combined with slave ATM switch, supports scalable integration of IP services over an ATM network. The MPLS LSC enables the slave ATM switch to do the following:

- Participate in an MPLS network
- Directly peer with IP routers
- Support the IP features in Cisco IOS software

The MPLS LSC supports highly scalable integration of MPLS (IP+ATM) services by using a direct peer relationship between the ATM switch and MPLS routers. This direct peer relationship removes the limitation on the number of IP edge routers (typical of traditional IP-over-ATM networks), allowing service providers to meet growing demands for IP services. The MPLS LSC also supports direct and rapid implementation of advanced IP services over ATM networks using ATM switches.

MPLS combines the performance and VC capabilities of Layer 2 (data link layer) switching with the scalability of Layer 3 (network layer) routing capabilities. This combination enables service providers to deliver solutions for managing growth, providing differentiated services, and leveraging existing networking infrastructures.

The MPLS LSC architecture provides the following flexibility:

- Run applications over any combination of Layer 2 technologies
- Support any Layer 3 protocol while scaling the network to meet future needs

By deploying the MPLS LSC across large enterprise networks or wide area networks, you can achieve the following benefits:

- Save money by using existing ATM and routing infrastructures
- Grow revenue using MPLS-enabled services
- Increase productivity through enhanced network scalability and performance

MPLS LSC Functional Description

The MPLS LSC is an LSR that is configured to control the operation of a separate ATM switch. Together, the MPLS LSC and the controlled ATM switch function as a single ATM MPLS router (ATM-LSR).

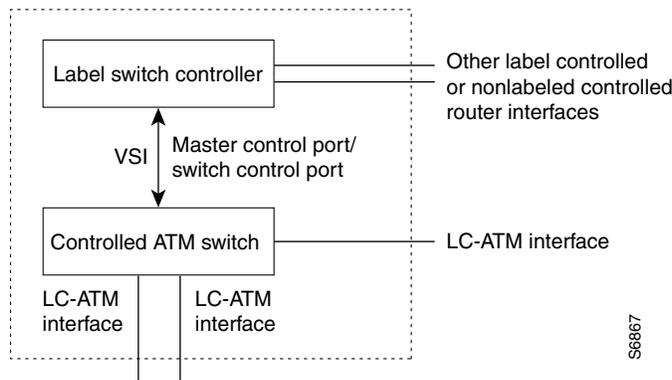
[Figure 36](#) shows the functional relationship between the MPLS LSC and the ATM switch that it controls.

Figure 36 *MPLS Label Switch Controller and Controlled ATM Switch*

The following routers can function as an MPLS LSC:

- Cisco 7200 series router
- Cisco 6400 Universal Access Concentrator (UAC)

The following ATM switches can function with the Cisco 7200 series router as the controlled ATM switch:



- Cisco BPX 8600, 8650 (which includes a Cisco 7204 router), and 8680
- Cisco IGX 8410, 8420, and 8430

**Note**

QoS is not an available feature with the IGX series ATM switches.

The MPLS LSC controls the ATM switch by means of the VSI, which runs over an ATM link connecting the two devices.

The dotted line in [Figure 36](#) represents the logical boundaries of the external interfaces of the MPLS LSC and the controlled ATM switch, as discovered by the IP routing topology. The controlled ATM switch provides one or more XTagATM interfaces at this external boundary. The MPLS LSC can incorporate other label controlled or nonlabel controlled router interfaces.

MPLS LSC benefits are as follows:

- IP-ATM integration—Enables ATM switches to directly support advanced IP services and protocols, thereby reducing operational costs and bandwidth requirements, while at the same time decreasing time-to-market for new services.
- Explicit routing—Provides Layer 2 VCs to gigabit router backbones and integrated IP+ATM environments, including support for explicit routing and provisioning of IP VPN services.
- SVPNs—Supports IP-based VPNs on either a Frame Relay or ATM backbone, an integrated IP-ATM backbone, or a gigabit router backbone.

Using Controlled ATM Switch Ports as Router Interfaces

In the LSC, the XTagATM ports on the controlled ATM switch are used as a Cisco IOS interface type called extended Label ATM (XTagATM). To associate these XTagATM interfaces with particular physical interfaces on the controlled ATM switch, use the **extended-port** interface configuration command.

[Figure 37](#) shows a typical MPLS LSC configuration that controls three ATM ports on a Cisco BPX switch: ports 6.1, 6.2, and 12.2. These corresponding XTagATM interfaces were created on the MPLS LSC and associated with the corresponding ATM ports on the Cisco BPX switch by means of the **extended-port** command.

Figure 37 Typical MPLS LSC and BPX Configuration

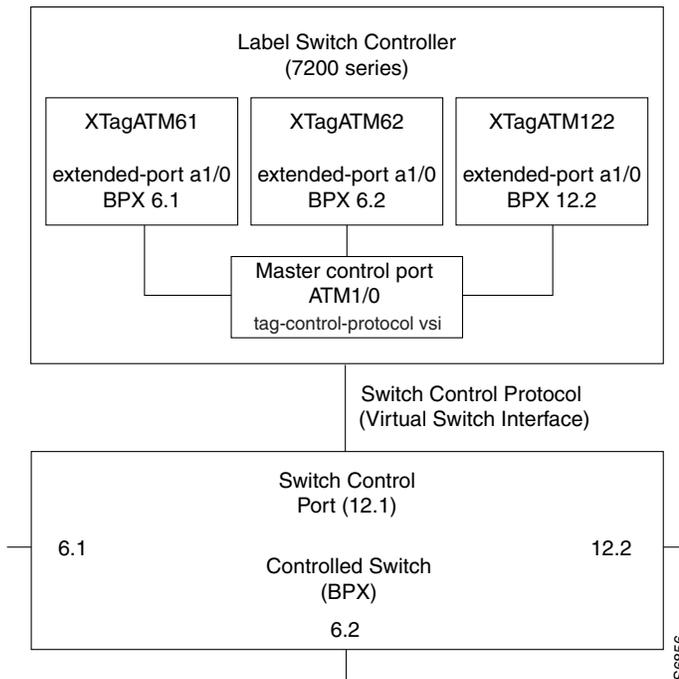


Figure 37 shows the following:

- An additional port on the Cisco BPX switch (port 12.1) acts as the switch control port
- An ATM interface (ATM1/0) on the MPLS LSC acts as the master control port

Using the MPLS LSC as a Label Edge Device



Note

Using the MPLS LSC as a label edge device is *not* recommended. Using the MPLS LSC as a label edge device introduces unnecessary complexity to the configuration. Refer to the **tag-switching atm disable-headend-vc** command in the *Cisco IOS Switching Services Command Reference* to disable edge LSR functionality on the LSC.

The MPLS LSC can perform as label edge device for the following purposes:

- Function simultaneously as a controller for an ATM switch and as a label edge device. Traffic can be forwarded between a router interface and an interface on the controlled switch, and between two XTagATM interfaces on the controlled switch.
- Perform label imposition and disposition and serve as the headend or tailend of a label-switched path tunnel.

However, when the MPLS LSC acts as a label edge device, it is limited by the following factors:

- Label space for LSC-terminated VCs is limited by the number of VCs supported on the control link.
- Packets are process switched between the LSC edge and an XTagATM interface.
- Throughput depends on the following factors:
 - The slave switch VSI partition configuration of the maximum cells per second for the master control port interface and the XTagATM interface.

- SAR limitations of the ATM Lite (PA-A1) and ATM Deluxe (PA-A3) and process switching.
- CPU utilization for the LSC and edge LSR functionality.

Creating Virtual Trunks

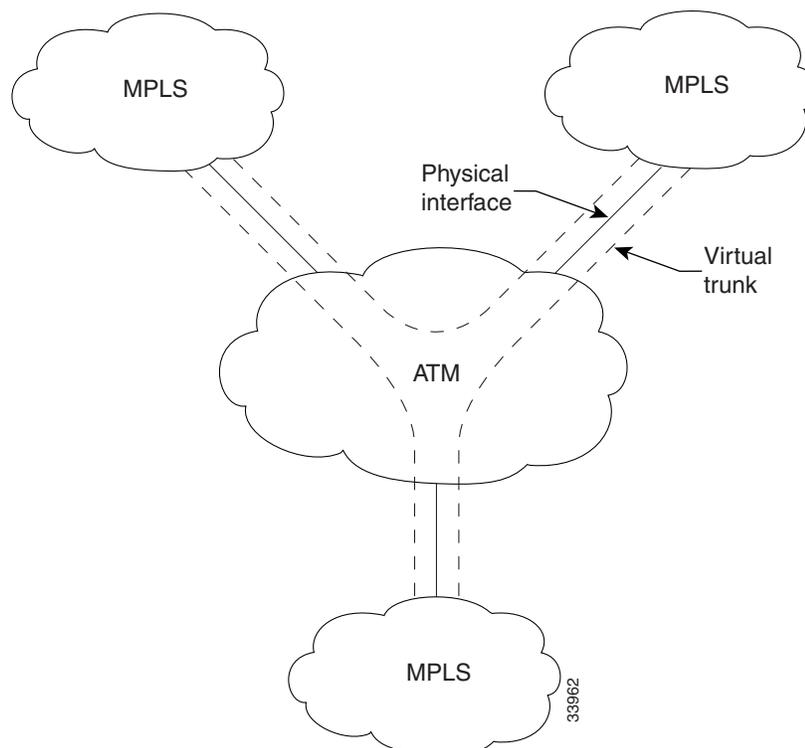
Virtual trunks provide connectivity for Cisco WAN MPLS switches through an ATM cloud, as shown in [Figure 38](#). Because several virtual trunks can be configured across a given private or public physical trunk, virtual trunks provide a cost-effective means of connecting across an entire ATM network.

The ATM equipment in the cloud must support virtual path switching and transmission of ATM cells based solely on the VPI in the ATM cell header. The VPI is provided by the ATM cloud administrator (that is, by the service provider).

Typical ATM Hybrid Network with Virtual Trunks

[Figure 38](#) shows three Cisco WAN MPLS switching networks, each connected to an ATM network by a physical line. The ATM network links all three of these subnetworks to every other subnetwork with a fully meshed network of virtual trunks. In this example, each physical interface is configured with two virtual trunks.

Figure 38 Typical ATM Hybrid Network Using Virtual Trunks



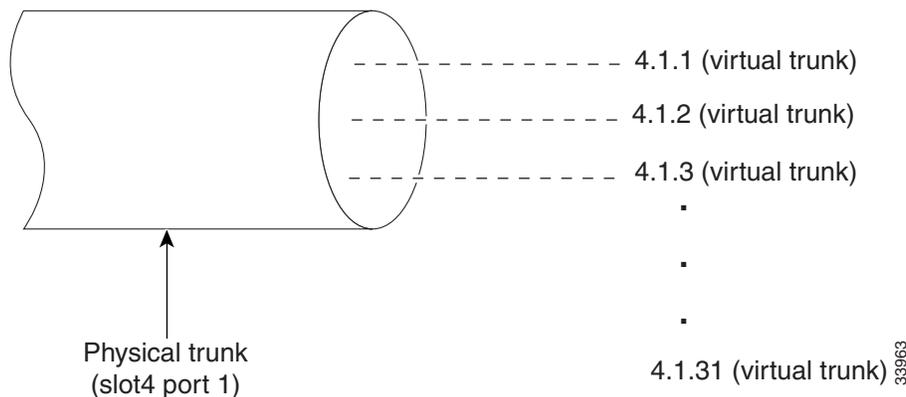
Benefits of virtual trunks are as follows:

- Reduced costs—By sharing the resources of a single physical trunk among a number of virtual (logical) trunks, each of the virtual trunks provided by the public carrier needs to be assigned only as much bandwidth as needed for that interface, rather than the full T3, E3, OC-3, or OC-12 bandwidth of an entire physical trunk.
- Migration of MPLS services into existing networks—VSI virtual trunks allow MPLS services to be carried over part of a network that does not support MPLS services. The part of the network that does not support such services may be a public ATM network, for example, that consists of switches that are not MPLS-enabled.

Virtual Trunk Configuration

A virtual trunk number (slot number.port number.trunk number) differentiates the virtual trunks found within a physical trunk port. In Figure 39, three virtual trunks (4.1.1, 4.1.2, and 4.1.3) are configured on a physical trunk that connects to the port 4.1 interface of a BXM switch.

Figure 39 Virtual Trunks Configured on a Physical Trunk



These virtual trunks are mapped to the XTagATM interfaces on the LSC. On the XTagATM interface, you configure the respective VPI value using the **tag-switching atm vp-tunnel vpi** interface command. This VPI should match the VPI in the ATM network. The LVCs are generated inside this Virtual Path (VP), and this VP carries the LVCs and their traffic across the network.

Virtual Trunk Bandwidth

The total bandwidth of all the virtual trunks on one port cannot exceed the maximum bandwidth of the port. Trunk loading (units of load) is maintained per virtual trunk, but the cumulative loading of all virtual trunks on a port is restricted by the transmit and receive rates for the port.

Virtual Trunk Features

The maximum number of virtual trunks that can be configured per card equals the number of virtual interfaces on the BPX or IGX switch. The following lists virtual interface support for BXM and UXM:

- The BXM supports 32 virtual interfaces; hence, it supports up to 32 virtual trunks. Accordingly, you can have interfaces ranging from XTagATM411 to XtagATM4131 on the same physical interface.
- The UXM supports 16 virtual interfaces. You can have interfaces ranging from XTagATM411 to XTagATM 4116.

Using LSC Redundancy

The following sections explain how LSC redundancy works:

- [LSC Redundancy Architecture](#)
- [General Redundancy Operational Modes](#)
- [How LSC Redundancy Differs from Router and Switch Redundancy](#)
- [How the LSC, ATM Switch, and VSI Work Together](#)
- [Implementing LSC Redundancy](#)
- [Reducing the Number of LVCs for LSC Redundancy](#)

LSC Redundancy Architecture

LSC redundancy allows you to create a highly reliable IP network, one whose reliability is nearly equivalent to that provided by Hot Standby routing. Instead of using Hot Standby routing processes to create redundancy, this method uses a combination of LSCs, the VSI, and IP routing paths with the same cost path for hot redundancy, or different costs for warm redundancy. The VSI allows multiple control planes (MPLS, Private Network-Network Interface (PNNI), and voice) to control the same switch. Each control plane controls a different partition of the switch.

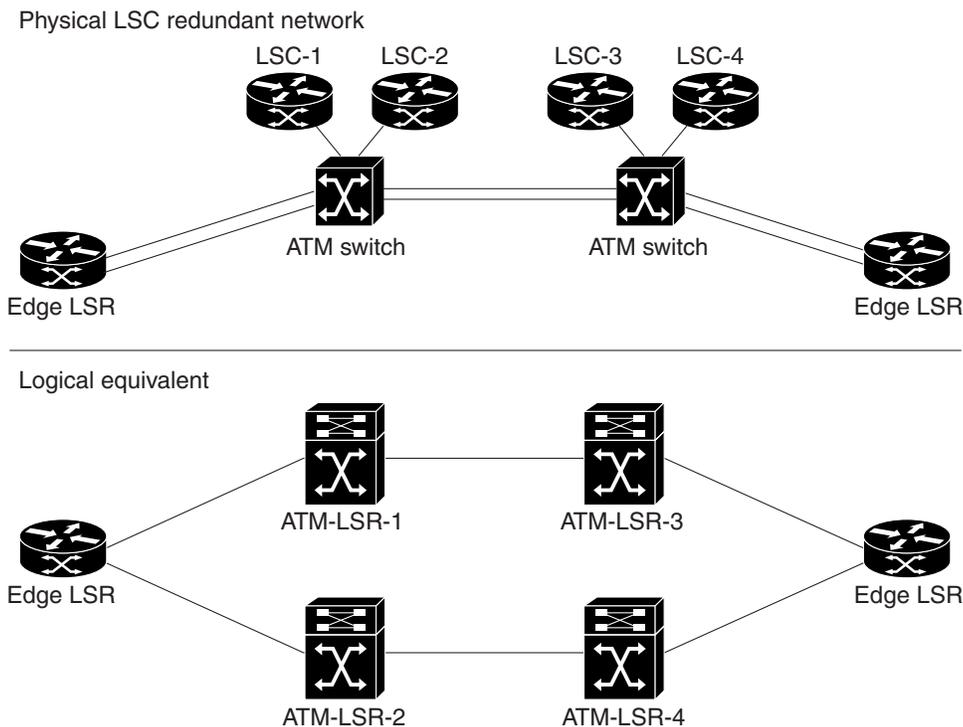
In the LSC redundancy model, two independent LSCs control the different partitions of the switch. Thus, two separate MPLS control planes set up connections on different partitions of the same switch. This is where LSC redundancy differs from Hot Standby redundancy: the LSCs do not need copies of the other internal state to create redundancy; the LSCs control the partitions of the switch independently.

A single IP network consists of switches with one LSC (or a Hot Standby pair of LSCs) and MPLS edge LSRs.

If you change that network configuration by assigning two LSCs per switch, you form two separate MPLS control planes for the network. You logically create two independent parallel IP subnetworks linked at the edge.

If the two LSCs on each switch are assigned identical shares of switch resources and links, the two subnetworks are identical. You have two identical parallel IP subnetworks on virtually the same equipment, which would otherwise support only one network.

For example, [Figure 40](#) shows a network of switches that each have two LSCs. MPLS edge LSRs are located at the edge of the network, to form a single IP network. The LSCs on each switch have identical shares of switch resources and links, which makes the networks identical. In other words, there are two identical parallel IP subnetworks.

Figure 40 LSC Redundancy Model

Part of the redundancy model includes edge LSRs, which link the two networks at the edge.

If the network uses OSPF or a similar IP routing protocol with an equal cost on each path, then there are at least two equally viable paths from every edge LSR to every other edge LSR. The OSPF equal-cost multipath distributes traffic evenly on both paths. Therefore, MPLS sets up two identical sets of connections for the two MPLS control planes. IP traffic travels equally across the two sets of connections.

**Note**

The LSC redundancy model works with any routing protocol. For example, you can use OSPF or IS-IS. Also, you can use both the TDP and the LDP.

With the LSC redundancy model, if one LSC on a switch fails, IP traffic uses the other path, without needing to establish new links. LSC redundancy does not require the network to set up new connections when a controller fails. Because the connections to the other paths have already been established, the interruption to the traffic flow is negligible. The LSC redundancy model is as reliable as networks that use Hot Standby controllers. LSC redundancy requires hardware like that used by Hot Standby controllers. However, the controllers act independently, rather than in Hot Standby mode. For LSC redundancy to work, the hardware must have connection capacity for doubled-up connections.

If an LSC fails and LSC redundancy is not present, IP traffic halts until other switches break their present connections and reroute traffic around the failed controller. The stopped IP traffic results in undesirable unreliability.

General Redundancy Operational Modes

The LSC redundancy model allows you to use the following four operational models. Most other redundancy models cannot accommodate all of these redundancy models.

- **Transparent Mode**—The primary and secondary redundant systems have the same copies of the image and startup configurations. When one system fails, the other takes over, and the operations are identical. However, this mode risks software failures, because both systems use the same algorithms. A software problem on the primary system is likely to affect the secondary system as well.
- **Upgrade mode**—You can upgrade the image or configuration of the redundant system, without rebooting the entire system. You can use this mode to change the resources between different partitions of the slave ATM switch.
- **Nontransparent mode**—The primary and secondary systems have different images or configurations. This mode is more reliable than transparent mode, which loads the same software on both controllers. In nontransparent mode, the use of different images and configurations reduces the risk of both systems encountering the same problem.
- **Experimental mode**—You load an experimental version of the image or configuration on the secondary system. You can use experimental mode when you want to test the new images in a real environment.

How LSC Redundancy Differs from Router and Switch Redundancy

In traditional IP router networks, network managers ensure reliability by creating multiple paths through the network from every source to every destination. If a device or link on one path fails, IP traffic uses an alternate path to reach its destination.

Router Redundancy

Because routers need not establish a VC to transfer data, they are inherently connectionless. When a router discovers a failed device or link, it requires approximately less than 1 second to reroute traffic from one path to another.

Routers can incorporate a warm or Hot Standby routing process to increase reliability. The routing processes share information about the routes to direct different streams of IP traffic. They need not keep or share connection information. Routers can also include redundant switch fabrics, backplanes, power supplies, and other components to decrease the chances of node failures.

ATM, Frame Relay, and Circuit Switch Redundancy

ATM, Frame Relay, and circuit switch networks transfer data by establishing circuits or VCs. To ensure the transfer of data in switches, network managers incorporate redundant switch components. If any component fails, a spare component takes over. Switches can have redundant line cards, power supplies, fans, backplanes, switch fabrics, line cards, and control cards. The following describes these redundant components:

- The redundant backplanes include all the hardware to operate two backplanes and to switch to the backup backplane if one fails.
- Redundant line cards protect against failed links. If a link to a line card fails, the redundant line card takes over. To create redundant line cards, you must program the same connection information into both line cards. This ensures that the circuits or VCs are not disrupted when the new line card takes over.
- The redundant switch fabric must also have the same connection information as the active switch fabric.

A software application usually monitors the state of the switches and their components. If a problem arises, the software sets an alarm to bring attention to the faulty component.

The redundant switch hardware and software are required, because switches take some time to reroute traffic when a failure occurs. Switches can have connection routing software, such as Cisco automatic connection routing, PNNI, or MPLS. However, rerouting the connections in a switch takes much more time than rerouting traffic in a router network. Rerouting connections in a switch requires calculating routes and reprogramming some hardware for each connection. In router networks, large aggregates of traffic can be rerouted simultaneously, with little or no hardware programming. Therefore, router networks can reroute traffic more quickly and easily than connection oriented networks. Router networks rely on rerouting techniques to ensure reliability. Connection-oriented networks use rerouting only as a last resort.

General Hot/Warm Standby Redundancy in Switches

Network managers can install redundant copies of the connection routing software for ATM and Frame Relay switches on a redundant pair of control processors.

With Hot Standby redundancy, the active process sends its state to the spare process to keep the spare process up to date in case it needs to take over. The active process sends the state information to the spare process or writes the state to a disk, where both processes can access the information. In either case, the state information is shared between controllers. Because the state of the network routing tables changes frequently, the software must perform much work to maintain consistent routing states between redundant pairs of controllers.

With Warm Standby redundancy, the state information is not shared between the active and spare processes. If a failure occurs, the spare process resets all of the connections and reestablishes them. Reliability decreases when the spare resets the connections. The chance of losing data increases.

LSC Redundancy

Connecting two independent LSCs to each switch by the VSI creates two identical subnetworks. Multipath IP routing uses both subnetworks equally. Thus, both subnetworks have identical connections. If a controller in one subnetwork fails, the multipath IP routing diverts traffic to the other path. Because the connections already exist in the alternate path, the reroute time is very fast. The LSC redundancy model matches the reliability of networks with Hot Standby controllers, without the difficulty of implementing Hot Standby redundancy.

One benefit of implementing the LSC redundancy model is that you eliminate the single point of failure between the LSC and the ATM switch it controls. If one LSC fails, the other LSC takes over and routes the data on the other path. The following sections explain the other benefits of LSC redundancy.

LSC Redundancy Does Not Use Shared States or Databases

In the LSC redundancy model, the LSCs do not share states or databases, which increases reliability. Sometimes, when states and databases are shared, an error in the state or database information can cause both controllers to fail simultaneously.

Also, new software features and enhancements do not affect LSC redundancy. Because the LSCs do not share states or database information, you need not worry about ensuring redundancy during every step of the update.

LSC Redundancy Allows Different Software Versions

The LSCs work independently and there is no interaction between the controllers. They do not share the state or database of the controller, as other redundancy models require. Therefore, you can run different versions of the Cisco IOS software on the LSCs, which provides the following advantages:

- You can test the features of the latest version of software without risking reliability. You can run the latest version of the Cisco IOS software on one LSC and an older version of the Cisco IOS software on a different LSC. If the LSC running the new Cisco IOS software fails, the LSC running the older software takes over.
- Running different versions of the Cisco IOS software reduces the chance of having both controllers fail. If you run the same version of the Cisco IOS software on both controllers and that version contains a problem, it could cause both controllers to fail. Running different versions on the controllers eliminates the possibility of each controller failing because of the same problem.

**Note**

Using different Cisco IOS software version on different LSCs is recommended only as a temporary measure. Different versions of Cisco IOS software in a network could be incompatible, although it is unlikely. For best results, run the same version of Cisco IOS software on all devices.

LSC Redundancy Allows Different Hardware

You can use different models of routers in this LSC redundancy model. For example, one LSC can be a Cisco 7200 series router, and the other LSC can be a Cisco 7500 series router. Using different hardware in the redundancy model reduces the chance that a hardware fault would interrupt network traffic.

LSC Redundancy Allows You to Switch from Hot to Warm Redundancy Immediately

You can implement hot or warm redundancy and switch from one model to the other. Hot redundancy can use redundant physical interfaces, slave ATM switches with Y redundancy, and redundant LSCs to enable parallel paths and near-instant failover. If your resources are limited, you can implement warm redundancy, which uses only redundant LSCs. When one controller fails, the backup controller requires some reroute time. As your network grows, you can switch from hot to warm redundancy and back, without bringing down the entire network.

Other redundancy models require complex hardware and software configurations, which are difficult to alter when you change the network configuration. You must manually change the connection routing software from Hot Standby mode to Warm Standby mode.

LSC Redundancy Provides an Easy Migration from Standalone LSCs to Redundant LSCs

You can migrate from a standalone LSC to a redundant LSC and back again without affecting network operations. Because the LSCs work independently, you can add a redundant LSC without interrupting the other LSC.

LSC Redundancy Allows Configuration Changes in a Live Network

The hot LSC redundancy model provides two parallel, independent networks. Therefore, you can disable one LSC without affecting the other LSC. This feature has the following benefits:

- LSC redundancy model facilitates configuration changes and updates. After you finish with configuration changes or image upgrades to the LSC, you can add it back to the network and resume the LSC redundancy model.
- The redundancy model protects the network during partitioning of the ATM switch. You can disable one path and perform partitioning on that path. While you are performing the partitioning, data uses the other path. The network is safe from the effects of the partitioning, which include breaking or establishing LVC connections.

LSC Redundancy Provides Fast Reroute in IP+ATM Networks

The hot LSC redundancy model offers redundant paths for every destination. Therefore, reroute recovery is very fast. Other rerouting processes in IP+ATM networks require many steps and take longer to reroute.

In normal IP+ATM networks, the reroute process consists of the following steps:

- Detecting the failure
- Converging the Layer 2 routing protocols
- Completing label distribution for all destinations
- Establishing new connections for all destinations

After this reroute process, the new path is ready to transfer data. Rerouting data using this process takes time.

The hot LSC redundancy method allows you to quickly reroute data in IP+ATM networks without using the normal reroute process. When you incorporate hot LSC redundancy, you create parallel paths. Every destination has at least one alternative path. If a device or link along the path fails, the data uses the other path to reach its destination. The hot LSC redundancy model provides the fastest reroute recovery time for IP+ATM networks.

How the LSC, ATM Switch, and VSI Work Together

In an LSC implementation, the LSC and slave ATM switch have the following characteristics:

- The LSC runs all of the control protocols.
- The ATM switch forwards the data.
- Each physical interface on the slave ATM switch maps to an XTagATM interface on the LSC. Each XTagATM interface has a dedicated LDP session with a corresponding interface on the edge. The XTagATM interfaces are mapped in the routing topology, and the ATM switch behaves as a router.
- The LSC can also function as an edge LSR. The data for the edge LSR passes through the control interface of the router.

If a component on the LSC fails, the IP switching function of the ATM switch is disabled. The standalone LSC is the single point of failure.

The VSI implementation includes the following characteristics:

- The VSI allows multiple, independent control planes to control a switch. The VSI ensures that the control processes (Signaling System 7 (SS7), MPLS, PNNI, and so on) can act independently of each other by using a VSI slave process to control the resources of the switch and apportion them to the correct control planes.
- In MPLS, each physical interface on the slave ATM switch maps to an XTagATM interface on the LSC through the VSI. In other words, physical interfaces are mapped to their respective logical interfaces.
- The routing protocol on the LSC generates route tables entries. The master sends connection requests and connection release requests to the slave.
- The slave sends the configured bandwidth parameters for the ATM switch interface to the master in the VSI messages. The master includes the bandwidth information in the link-state topology. You can override these bandwidth values by manually configuring the bandwidth on the XTagATM interfaces.

Implementing LSC Redundancy

To make an LSC redundant, you can partition the resources of the slave ATM switch, implement a parallel VSI model, assign redundant LSCs to each switch, and create redundant LSRs. The following sections explain these steps.

Partitioning the Resources of the ATM Switch

In the LSC redundancy model, two LSCs control different partitions of the ATM switch. When you partition the ATM switch for LSC redundancy, use the following guidelines:

- Make the MPLS partitions identical. If you create two partitions, make sure both partitions have the same amount of resources. (You can have two MPLS VSI partitions per switch.) Use the **cnfrsrc** router configuration command to configure the partitions.
- If the partitions are on the same switch card, perform the following steps:
 - Create different control VCs for each partition. For example, there can be only one (0, 32) control VC on the XTagATM interface. To map two XTagATM interfaces on the same ATM switch interface, use a different control VC for the second LSC. Use the **tag-switching atm control-vc** interface command.
 - Create the LVC on the XTagATM interfaces using nonintersecting VPI ranges. Use the **tag-switching atm vpi** interface command.
- Specify the bandwidth information on the XTagATM interfaces. Normally, this information is read from the slave ATM switch. When you specify the bandwidth on the XTagATM interface, the value you enter takes precedence over the switch-configured interface bandwidth.
- Configure the logical channel number (LCN) ranges for each partition according to the expected number of connections.

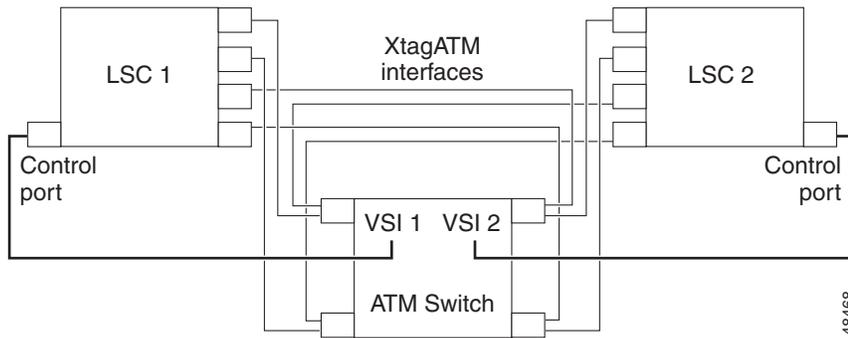
See the documentation on the Cisco BPX 8600 series or Cisco IGX 8400 series switches for more information about configuring the slave ATM switch.

Implementing the Parallel VSI Model

The parallel VSI model means that the physical interfaces on the ATM switch are shared by more than one LSC. For instance, LSC1 in [Table 26](#) maps VSI slave interfaces 1 to N to the ATM switch physical interfaces 1 to N. LSC2 maps VSI slave interfaces to the ATM switch's physical interfaces 1 to N. LSC1 and LSC2 share the same physical interfaces on the ATM switch. With this mapping, you achieve fully meshed independent masters.

[Figure 41](#) shows four ATM physical interfaces mapped as four XTagATM interfaces at LSC1 and LSC2. Each LSC is not aware that the other LSC is mapped to the same interfaces. Both LSCs are active all the time. The ATM switch runs the same VSI protocol on both partitions.

Figure 41 XTagATM Interfaces

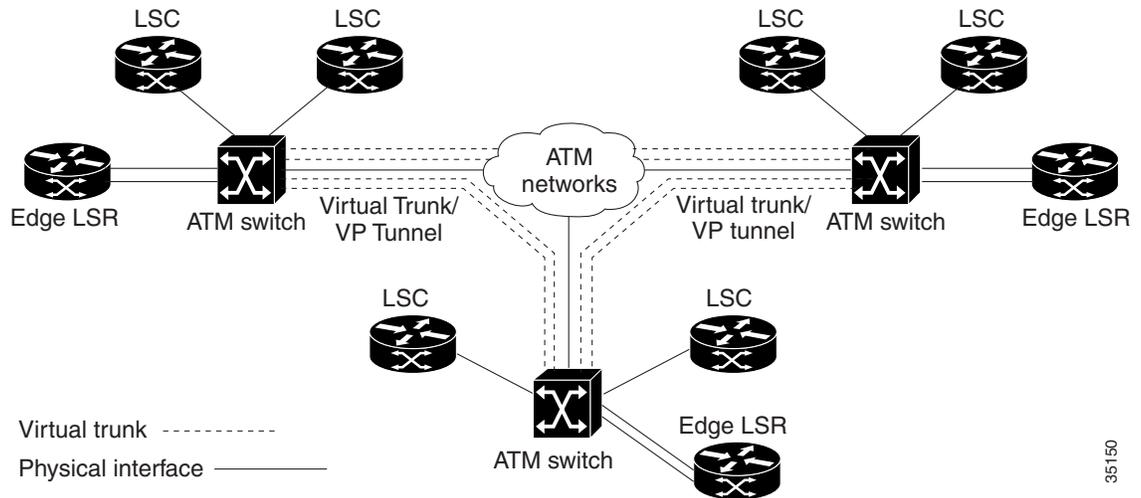


Adding Interface Redundancy

To ensure reliability throughout the LSC redundant network, you can also implement:

- Redundant interfaces between the edge LSR and the ATM-LSR. Most edge LSRs are collocated with the LSCs. Creating redundant interfaces between the edge LSRs and the ATM LSRs reduces the chance of a disruption in network traffic by providing parallel paths.
- Redundant virtual trunks and VP tunnels between slave ATM switches. To ensure hot redundancy between the ATM switches, you can create redundant virtual trunks and VP tunnels. See Figure 42.

Figure 42 Interface Redundancy



Implementing Hot or Warm LSC Redundancy

Virtually any configuration of switches and LSCs that provides hot redundancy can also provide warm redundancy. You can also switch from warm to hot redundancy with little or no change to the links, switch configurations, or partitions.

Hot and warm redundancy differ in the following ways:

- Hot redundancy uses both paths to route traffic. You set up both paths using equal-cost multipath routing, so that traffic is load balanced between the two paths. As a result, hot redundancy uses twice the number of MPLS label VCs as warm redundancy.

- Warm redundancy uses only one path at a time. You set up the paths so that one path has a higher cost than the other. Traffic only uses one path and the other path is a backup path.

The following sections explain the two redundancy models in detail.

Implementing Hot LSC Redundancy

Hot redundancy provides near-instant failover to the other path when an LSC fails. When you set up hot redundancy, both LSCs are active and have the same routing costs on both paths. To ensure that the routing costs are the same, run the same routing protocols on the redundant LSCs.

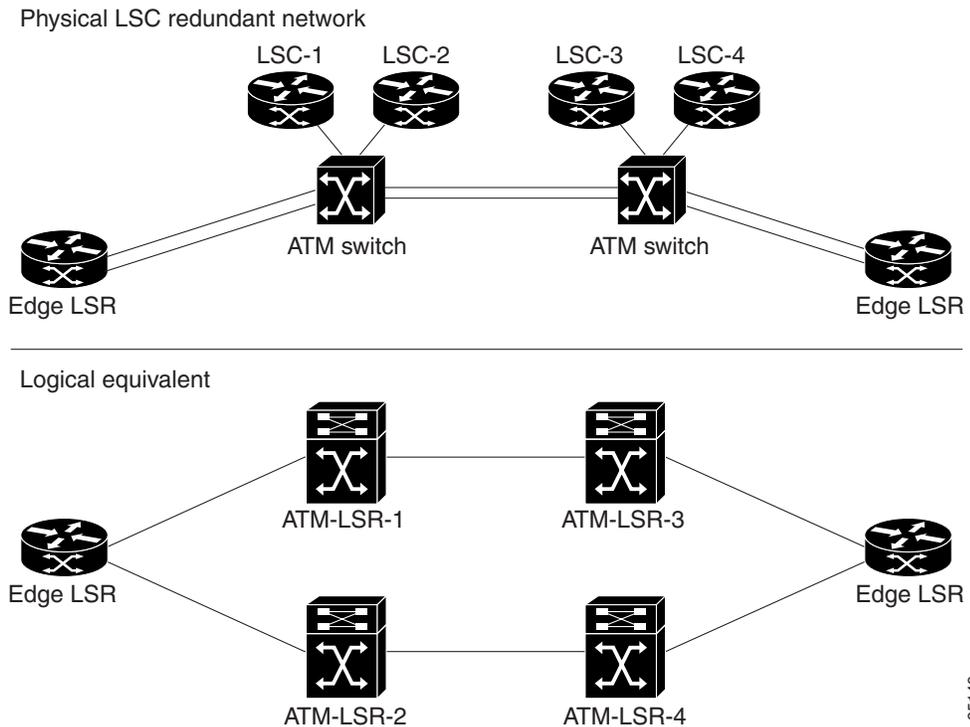
In hot redundancy, the LSCs run parallel and independent LDPS. At the edge LSRs, when the LDP has multiple routes for the same destination, it requests multiple labels. It also requests multiple labels when it needs to support QoS. When one LSC fails, the labels distributed by that LSC are removed.

To achieve hot redundancy, you can implement the following redundant components:

- Redundant physical interfaces between the edge LSR and the ATM-LSR to ensure reliability in case one physical interface fails.
- Redundant interfaces or redundant VP tunnels between the ATM switches.
- Slave ATM switches, such as the BPX 8650, can have redundant control cards and switch fabrics. If redundant switch fabrics are used and the primary switch fails, the other switch fabric takes over.
- Redundant LSCs.
- The same routing protocol running on both LSCs. (You can have different tag or label distribution protocols.)

Figure 43 shows one example of how hot LSC redundancy can be implemented.

Figure 43 Hot LSC Redundancy



35149

Implementing Warm LSC Redundancy

To achieve warm redundancy, you need only redundant LSCs. You need not run the same routing protocols or distribution protocols on the LSCs.



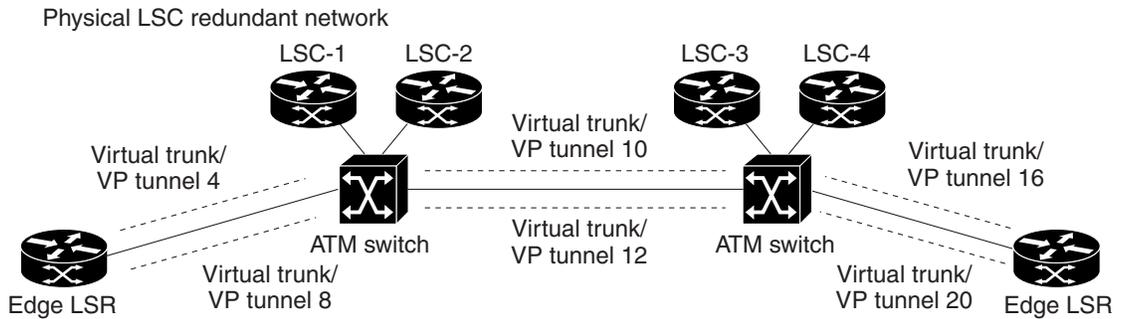
Note

You can use different routing protocols on parallel LSCs. However, you do not get near-instant failover. The failover time includes the time it takes to reroute the traffic, plus the LDP bind request time. If the primary routing protocol fails, the secondary routing protocol finds new routes and creates new LVCs. An advantage to using different routing protocols is that the ATM switch uses fewer resources and offers more robust redundancy.

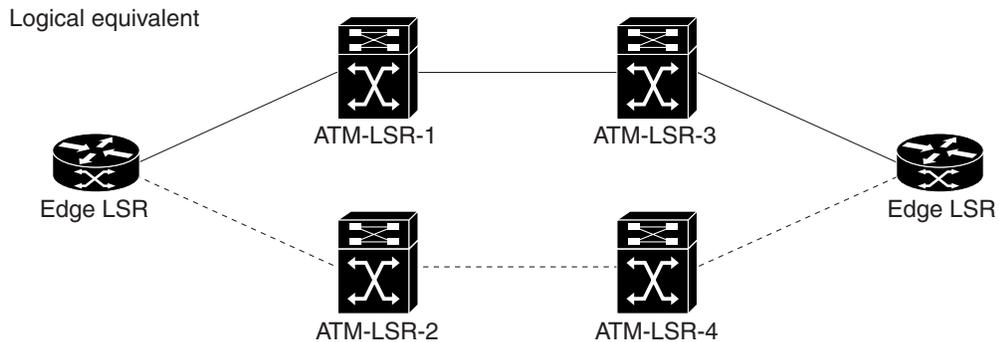
If you run the same routing protocols, specify a higher cost for the interfaces on the backup LSC to allow the data to use only the lower-cost path and also saves resources on the ATM switch (the edge LSR requests LVCs only through the lower-cost LSC). When the primary LSC fails, the edge LSR uses the backup LSC and creates new paths to the destination. Creating new paths requires reroute time and LDP negotiation time.

Figure 44 shows one example of how warm LSC redundancy can be implemented.

Figure 44 Warm LSC Redundancy



Note: Tunnels are virtual interfaces. -----
Physical interfaces are marked by thin lines. _____



35152

Reducing the Number of LVCs for LSC Redundancy

By default, an LSC includes edge LSR functionality, which means that the LSC can act as a label edge device. To achieve the edge LSR functionality, the LSC creates an LSP for each destination in the route table.

With LSC redundancy, if 400 destinations exist in the network, each redundant LSC adds 400 headend VCs. In hot redundancy mode, 800 headend VCs are created for the LSCs. If the LSCs are not edge LSRs, then 800 LVCs are wasted.

The number of LVCs increases as the number of redundant LSCs increases. In the case of a VC-merged system, the number of LVCs can be low. However, in non-VC-merged system, the number of LVCs can be high. To reduce the number of LVCs, disable the edge LSR functionality in the LSC. Enter the **tag-switching atm disable headend-vc** interface command to disable the edge LSR functionality on the LSC and prevent the creation of headend VCs.



Note

As an alternative to the **tag-switching atm disable headend-vc** interface command, you can issue the **tag-switching request-tags for** interface command with an access list to save LVC space.

For more information on reducing the number of LVCs, see the [“Reducing the Number of Label Switch Paths Created in an MPLS Network”](#) section.

Implementation Considerations

The following sections explain items that need to be considered when implementing hot or warm LSC redundancy in a network.

Hot LSC Redundancy Considerations

The following list explains the items you need to consider when implementing hot LSC redundancy:

- LSC hot redundancy needs parallel paths. Specifically, there must be the capacity for at least two end-to-end parallel paths traveling from each source to each destination. Each path is controlled by one of a pair of redundant LSCs.
- LSPs for the destinations are initiated from the edge LSR. The edge LSR initiates multiple paths for a destination only if it has parallel paths to its next hop. Therefore, it is important to have parallel paths from the edge LSR. You can achieve parallel paths by having two physical links from the edge LSR or by having two separate VP tunnels on one link.
- Hot redundancy protection extends from the edge LSR only as far as parallel paths are present. So, it is best if parallel paths are present throughout the entire network.
- Hot redundancy increases the number of VCs used in the network. Each physical link with two VSI partitions has twice the number of VCs used than would otherwise be the case. Various techniques can be used to alleviate VC usage. The use of unnumbered links (“ip unnumbered” in the Cisco IOS link configuration) reduces the number of routes in the routing table and hence the number of VCs required. On the LSCs, you can use the **tag-switching atm disable headend-vc** interface command to disable edge LSR functionality on the LSC and also reduce the number of VCs used. The **tag-switching request-tags for** interface command with an access list also restricts the creation of LVCs.

Warm LSC Redundancy Considerations

The following list explains the items you need to consider when implementing warm LSC redundancy:

- LSC warm redundancy needs a single active path between the source and destination. However, there is also a requirement for end-to-end parallel paths, as in the hot redundancy case. Only one path has an active LSP for the destination. In the event of the failure, the other path is established, with some delay due to rerouting.
- The number of VCs in the network does not change with the warm redundancy.
- Hot LSC redundancy achieves failure recovery with little loss of traffic. However, hot redundancy doubles the VC requirements in the network. Warm LSC redundancy requires the same number of VCs as a similar network without LSC redundancy. However, traffic loss due to a failure is greater; traffic may be lost for a period of seconds during rerouting.

**Note**

The precise traffic loss depends on the type of failure. If the failure is in an LSC, the LSPs controlled by that LSC typically remain connected for some time. Traffic can still flow successfully on the “failed” path until the edge LSRs switch all traffic to the alternate path (which might occur tens of seconds later, depending on routing protocol configuration). The only traffic loss might occur in the edge LSR when traffic changes to the new path, which typically takes a few milliseconds or less.

Reducing the Number of Label Switch Paths Created in an MPLS Network

You can use two methods to reduce the number of LSPs created in an MPLS network:

- Disable LSPs from being created from a edge LSR or LSC to a destination IP address. Use the **tag-switching request-tags for** interface command. Specify the destination IP addresses that you want to disable from creating LSPs. This command allows you to permit creation of some LSPs, while preventing the creation of others.
- Disable the LSC from acting as an edge LSR by using the **tag-switching atm disable headend-vc** interface command. This command removes all LSPs that originate at the MPLS LSC and disables the LSC from acting as an edge LSR.

Using an Access List to Disable Creation of LSPs to Destination IP Addresses

You can prevent LSPs from being created between edge LSRs and LSCs to prevent the unnecessary use of LVC resources in a slave ATM switch. Use the **tag-switching request-tags for** interface command with an access list to disable the creation of the LSPs.

Some LSPs are often unnecessary between some edge LSRs in an MPLS network. Every time a new destination is created, LSPs are created from all edge LSRs in the MPLS network to the new destination. You can create an access list at an edge LSR or LSC to restrict the destinations for which a downstream-on-demand request is issued.

For example, [Figure 45](#) is an MPLS ATM network that consists of the following elements:

- The PE routers in the VPN require LSPs to communicate with each other.
- All the PE routers are in network 1 (198.x.x.x).
- All the IGP IP addresses are in network 2 (192.x.x.x).
- If numbered interfaces are required (for network management or other purposes), they are placed in network 2 (192.x.x.x).

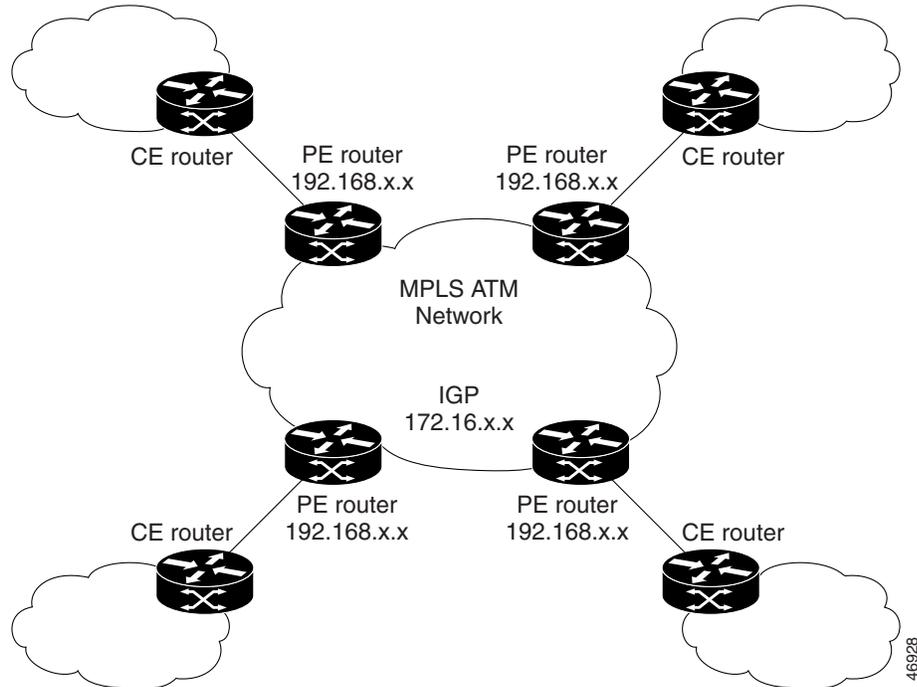
Use **tag-switching request-tags for** interface commands to accomplish the following tasks:

- Allow the PE routers in network 1 to create LSPs and communicate with each other.

- Prevent LSPs from being created in network 2.

Performing these tasks reduces the number of LSPs in the MPLS ATM cloud, which reduces the VC usage in the cloud.

Figure 45 Sample MPLS ATM Network

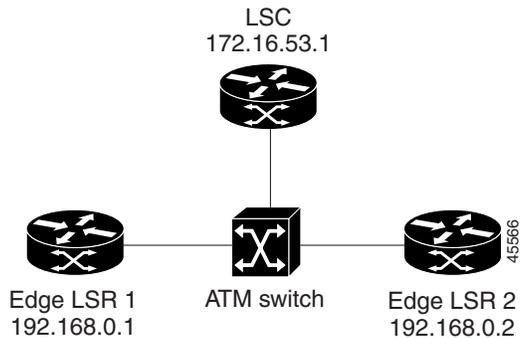


Note

When using access lists to prevent the creation of headend LVCs or LSPs, do not disable the LSC from acting as an edge LSR with the **tag-switching disable headend-vc** interface command, which prevents all LSPs from being established.

The following examples of the **tag-switching request tags-for** interface command use [Figure 46](#) as a basis. The examples show different ways to disable the creation of LSPs from the LSC to the edge LSR, and from the edge LSRs to the LSC.

Figure 46 **Sample Configuration**



Using a Numbered Access List

The following examples use a numbered access list to restrict creation of LSPs.

Preventing LSPs from the LSC to the Edge LSRs

The following example prevents LSPs from being established from the LSC to all 198.x.x.x destinations. However, transit LSPs are allowed between 198.x.x.x destinations. Add the following commands to the LSC configuration:

```
tag-switching request-tags for 1
access-list 1 deny 198.0.0.0 0.255.255.255
access-list 1 permit any
```

Preventing LSPs from the Edge LSRs to the LSC

The following example prevents headend LVCs from being established from edge LSR 1 and edge LSR 2 to the LSC (192.x.x.x). However, transit LSPs are allowed between 198.x.x.x destinations. Add the following commands to the edge LSR 1 and 2 configurations:

```
tag-switching request-tags for 1
access-list 1 deny 192.0.0.0 0.255.255.255
access-list 1 permit any
```

Using a Named Access List

The following examples use a named access list to perform the same tasks as in the previous examples:

```
tag-switching request-tags for nolervcs
ip access-list standard nolervcs
deny 198.0.0.0 0.255.255.255
permit any
```

```
tag-switching request-tags for nolervcs
ip access-list standard nolervcs
deny 192.0.0.0 0.255.255.255
permit any
```

Specifying Exact Match IP Addresses with an Access List

The following examples use exact IP addresses to perform the same tasks as in the previous examples:

```
tag-switching request-tags for 1
access-list 1 deny 198.5.0.1 0.0.0.0
access-list 1 deny 198.5.0.2 0.0.0.0
access-list 1 permit any
```

```
tag-switching request-tags for 1
access-list 1 deny 192.6.53.1 0.0.0.0
access-list 1 permit any
```

Instead of configuring an access list on the LSC, you can issue the **tag-switching atm disable-headend-vc** interface command to disable the creation of LSPs. This command works only with LSCs.

Disabling the LSC from Acting as an Edge LSR

To remove all LSPs from the MPLS LSC and disable its ability to function as an edge LSR, you can use either of the following interface commands:

- **tag-switching atm disable-headend-vc**
- **tag-switching request-tags for**

Disabling the LSC from acting as an edge LSR causes the LSC to stop initiating LSPs to any destination. Therefore, the number of LVCs used in the network is reduced. The LSC can still terminate tailend LVCs, if required.

With downstream on demand, LVCs are depleted with the addition of each new node. These commands save resources by disabling the LSC from setting up unwanted LSPs. The absence of those LSPs allows traffic to follow the same path as control traffic.

The following example uses the **tag-switching atm disable-headend-vc** interface command to disable the LSC from functioning as an edge LSR. The following line is added to the LSC configuration:

```
tag-switching atm disable-headend vc
```

The following example uses the **tag-switching request-tags for** interface command to disable the LSC from functioning as an edge LSR. The following lines are added to the LSC configuration:

```
tag-switching request-tags for dedicatedlsc
ip access-list standard dedicatedlsc
deny any
```



Note

For a Cisco 6400 UAC with an NRP configured to function as an LSC, disable the LSC from acting as an edge LSR. An NRP LSC should only support label switch paths through the controlled ATM switch under VSI control.

Using the Cisco 6400 Universal Access Concentrator as an MPLS LSC

You can configure the Cisco 6400 UAC to operate as an MPLS LSC in an MPLS network. The hardware that supports MPLS LSC functionality on the Cisco 6400 UAC is described in the following sections.

**Note**

If you configure a Cisco 6400 UAC with a node resource processor (NRP) to function as an LSC, disable MPLS edge LSR functionality. Refer to the **tag-switching atm disable-headend-vc** command in the *Cisco IOS Switching Services Command Reference* for information on disabling MPLS edge LSR functionality. An NRP LSC should support transit label switch paths only through the controlled ATM switch under VSI control.

Cisco 6400 UAC Architectural Overview

A Cisco 6400 UAC can operate as an MPLS LSC if it incorporates the following components:

- Node switch processor (NSP)—The NSP incorporates an ATM switch fabric, enabling the Cisco 6400 UAC to function as ATM-LSR in a network. The NSP manages all the external ATM interfaces for the Cisco 6400 UAC.
- NRP—The NRP enables a Cisco 6400 UAC to function as an LSC. When you use the NRP as an LSC, however, you must not configure the NRP to perform other functions.

The NRP contains internal ATM interfaces that enable it to be connected to the NSP. However, the NRP cannot access the external ATM interfaces of the Cisco 6400 UAC. Only the NSP can access the external ATM interfaces.

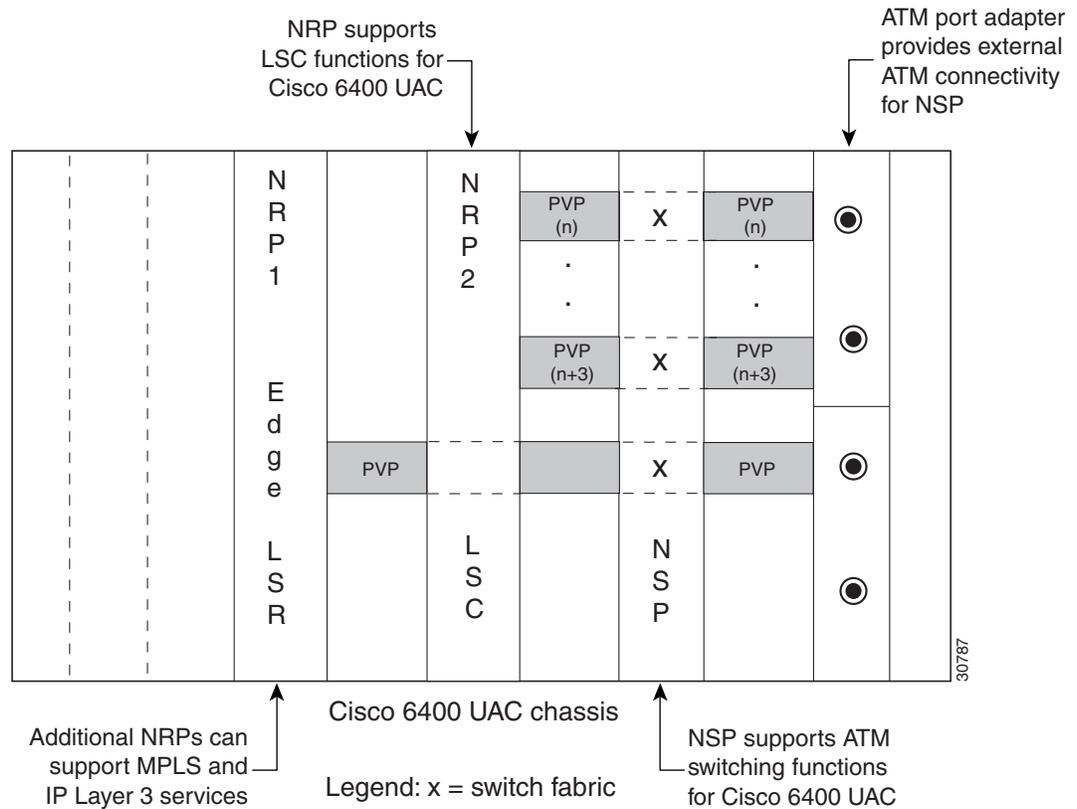
**Note**

A Cisco 6400 UAC chassis can accommodate multiple NRPs, including one dedicated to MPLS LSC functions. You cannot use an additional NRP as an MPLS LSC. However, you can use additional NRPs to run MPLS and perform other networking services.

- ATM port adapter—The Cisco 6400 UAC uses an ATM port adapter to provide external connectivity for the NSP.

Figure 47 shows the components that you can configure to enable the Cisco 6400 UAC to function as an MPLS LSC.

Figure 47 Cisco 6400 UAC Configured as an MPLS LSC



Configuring Permanent Virtual Circuits and Permanent Virtual Paths

The NRP controls the slave ATM switch through the VSI protocol. The VSI protocol operates over a PVC that you configure. The PVC is dedicated to the VCs that the VSI control channel uses.

For the NRP to control an ATM switch through the VSI, cross-connect the control VCs from the ATM switch through the NSP to the NRP. The ATM switch (BPX) uses defined control VCs for each BXM slot of the BPX chassis, enabling the LSC to control external XTagATM interfaces through the VSI.

[Table 27](#) defines the PVCs that must be configured on the NSP interface connected to the BPX VSI shelf. These PVCs are cross-connected via the NSP to the NRP VSI master control port, which is running the VSI protocol.

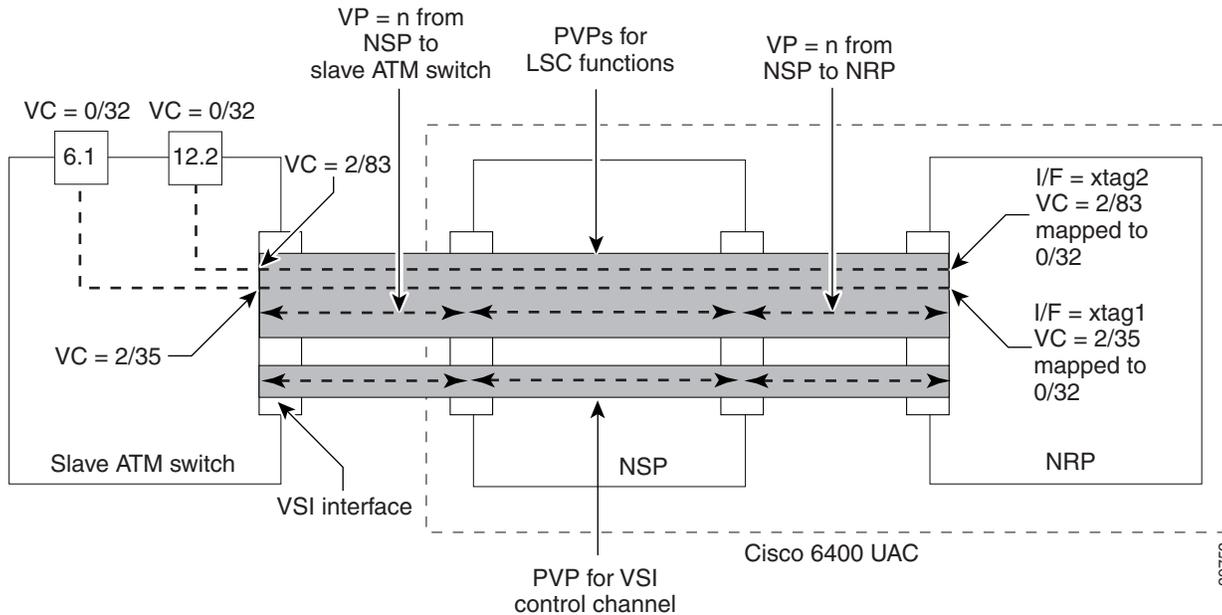
For an NRP that is installed in slot 3 of a Cisco 6400 UAC chassis, the master control port would be ATM3/0/0 on the NSP. As shown in [Figure 37](#), the BPX switch control interface is 12.1, and the NSP ATM port connected to this interface is the ATM interface that is cross-connected to ATM3/0/0. Because [Figure 37](#) shows that the BXM slaves in BPX slots 6 and 12 are configured as external XTagATM ports, the PVCs that must be cross-connected through the NSP are 0/45 for slot 6 and 0/51 for slot 12, respectively, as outlined in [Table 27](#).

Table 27 VSI Interface Control PVCs for BPX VSI Slave Slots

BPX VSI Slave Slot	VSI Interface Control VC
1	0/40
2	0/41
3	0/42
4	0/43
5	0/44
6	0/45
7	0/46
8	0/47
9	0/48
10	0/49
11	0/50
12	0/51
13	0/52
14	0/53

Figure 48 shows the functional relationships among the Cisco 6400 UAC hardware components and the permanent virtual paths (PVPs) that you can configure to support MPLS LSC functionality.

Figure 48 Cisco 6400 UAC PVP Configuration for MPLS LSC Functions



All other MPLS LSC functions, such as routing, terminating LVCs, and LDP control VCs (default 0/32), can be accomplished by means of a separate, manually configured PVP (see the upper shaded area in Figure 48). The value of “n” for this manually configured PVP must be the same among all the associated

devices (the NRP, the NSP, and the slave ATM switch). Because the NSP uses $VP = 0$ for ATM Forum signalling and the BPX uses $VP = 1$ for autoroute, the value of “n” for this PVP for MPLS LSC functions must be greater than or equal to 2, while not exceeding an upper bound.

Note that some edge LSRs have ATM interfaces with limited VC space per virtual path (VP). For these interface types, you define several VPs. For example, the Cisco ATM Port Adapter (PA-A1) and the AIP interface are limited to VC range 33 through 1018. To use the full capacity of the ATM interface, configure four consecutive VPs. Make sure the VPs are within the configured range of the BPX.

For internodal BPX connections, we suggest that you configure VPs 2 through 15; for edge LSRs, we suggest that you configure VPs 2 through 5. (Refer to the BPX **cnfrsrc** command in the *Cisco BPX 8600 Series* documentation for examples of how to configure BPX service nodes.)

Control VC Setup for MPLS LSC Functions

After you connect the NRP, the NSP, and the slave ATM switch by means of manually configured PVPs (as shown in [Figure 48](#)), the NRP can control the slave ATM switch as though it is directly connected to the NRP. The NRP discovers the interfaces of the slave ATM switch and establishes the default control VC to be used in creating MPLS VCs.

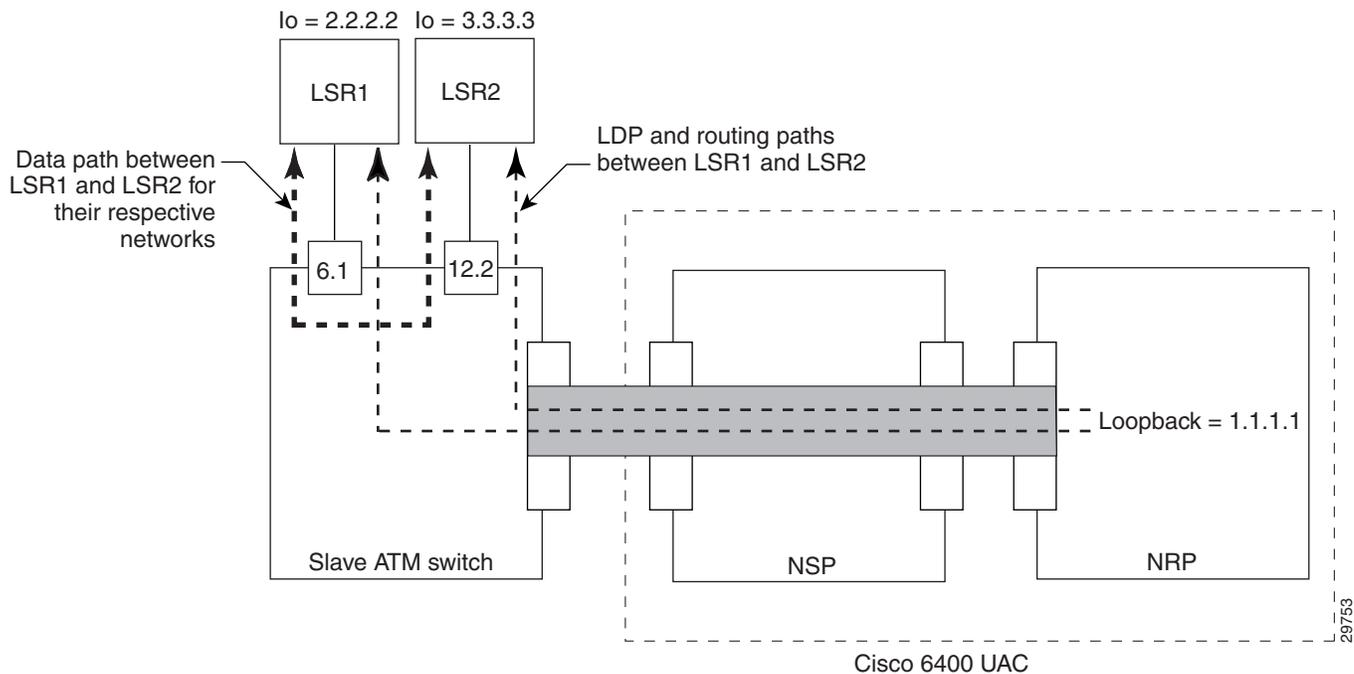
The slave ATM switch shown in [Figure 48](#) incorporates two external ATM interfaces (labeled xtag1 and xtag2) that are known to the NRP as XTagATM61 and XTagATM122, respectively. On interface 6.1 of the slave ATM switch, VC = 0/32 is connected to VC 2/35 by the VSI protocol. On the NRP, VC 2/35 is terminated on interface XTagATM61 and mapped to VC 0/32, also by means of the VSI protocol. This mapping enables the LDP to discover MPLS LSC neighbors by means of the default control VC 0/32 on the physical interface. On interface 12.2 of the slave ATM switch, VC 0/32 is connected to VC 2/83 by the VSI protocol. On the NRP, VC 2/83 is terminated on interface XTagATM122 and mapped to VC 0/32.

Note that the selection of these VCs is dependent on the availability of VC space. Hence it is not predictable which physical VC will be mapped to the external default control VC 0/32 on the XTagATM interface. The control VC will be shown as a PVC on the LSC, as opposed to an LVC, when you enter the Cisco IOS **show xtagatm vc EXEC** command.

Configuring the Cisco 6400 UAC to Perform Basic MPLS LSC Operations

[Figure 49](#) shows a Cisco 6400 UAC containing a single NRP that has been configured to perform basic MPLS LSC operations.

Figure 49 Typical Cisco 6400 UAC Configuration to Support MPLS LSC Functions



Note If the NRP incurs a fault that causes it to malfunction (in a single NRP configuration), the LVCs and routing paths pertaining to MPLS LSC functions are lost.



Note The loopback addresses must be configured with a 32-bit mask and be included in the relevant IGP or BGP routing protocol, as shown in the following example:

```
ip address 192.103.210.5 255.255.255.255
```

Defining the MPLS Control and IP Routing Paths

In the MPLS LSC topology shown in [Figure 49](#), the devices labeled LSR1 and LSR2 are external to the Cisco 6400 UAC. These devices, with loopback addresses as their respective LDP identifiers, are connected to two separate interfaces labeled 6.1 and 12.2 on the slave ATM switch. Both LSR1 and LSR2 learn about the routes of each other from the NRP by means of the data path represented as the thick dashed line in [Figure 49](#). Subsequently, LVCs are established by means of LDP operations to create the data paths between LSR1 and LSR2 through the ATM slave switch.

Both LSR1 and LSR2 learn of the loopback address of the NRP and create a data path (LVCs) from each other that terminates in the NRP. These LVCs, called tailend LVCs, are not shown in [Figure 49](#).

Disabling Edge LVCs

By default, the NRP requests LVCs for the next hop devices (the LSRs shown in [Figure 49](#)). The headend LVCs enable the LSC to operate as an edge LSR. Because the NRP is dedicated to the slave ATM switch by default, the headend LVCs are not required.

**Note**

If a Cisco 6400 UAC with an NRP is configured to function as an LSC, disable the edge LSR functionality. An NRP LSC should support transit LSPs only through the controlled ATM switch under VSI control. Refer to the **tag-switching atm disable-headend-vc** interface command in the *Cisco IOS Switching Services Command Reference* to disable edge LSR functionality.

The **tag-switching atm disable-headend-vc** command disables the default behavior of the NRP in setting up headend switch LVCs, thereby saving VC space.

Supporting ATM Forum Protocols

You can connect the MPLS LSC to a network that is running ATM Forum protocols while the MPLS LSC simultaneously performs its functions. However, you must connect the ATM Forum network through a separate ATM interface (that is, not through the master control port).

MPLS Egress NetFlow Accounting

MPLS egress NetFlow accounting allows you to capture IP flow information for packets undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS and are sent as IP.

Previous to the MPLS Egress NetFlow Accounting feature, you captured NetFlow data only for flows that arrived on the packet in IP format. When an edge router performed MPLS label imposition (received an IP packet and sent it as an MPLS packet), NetFlow data was captured when the packet entered the network. Inside the network, the packet was switched based only on MPLS information, and thus NetFlow information was not captured until after the last label was removed.

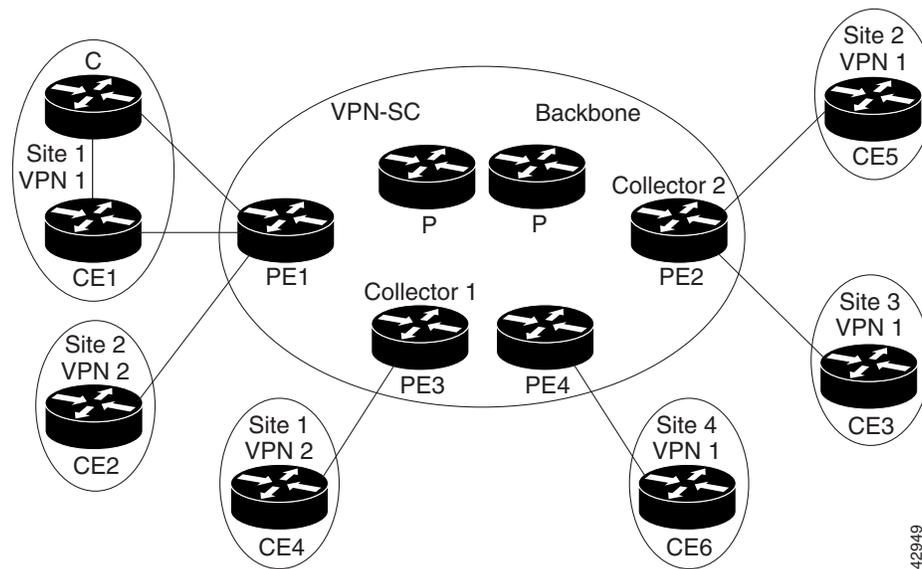
One common application of the MPLS egress NetFlow accounting feature allows you to capture the MPLS VPN IP flows that are traveling from one site of a VPN to another site of the same VPN through the service provider backbone.

Previous to the MPLS Egress NetFlow Accounting feature, you captured flows only for IP packets on the ingress interface of a router. You could not capture flows for MPLS encapsulated frames, which were switched through CEF from the input port. Therefore, in an MPLS VPN environment you captured flow information as packets were received from a CE router and forwarded to the backbone. However, you could not capture flow information as packets were sent to a CE router because those packets were received as MPLS frames.

The MPLS egress NetFlow accounting feature lets you capture the flows on the outgoing interfaces.

[Figure 50](#) shows a sample topology. To capture the flow of traffic going to Site 2 of VPN 1 from any remote VPN 1 sites, you enable MPLS egress NetFlow accounting on link PE2-CE5 of provider edge router PE2. The flows are stored in a global flow cache maintained by the router. You can use the **show ip cache flow EXEC** command or other aggregation flow commands to view the egress flow data.

Figure 50 Provider and Customer Networks with MPLS Egress NetFlow Accounting



The PE routers export the captured flows to the configured collector devices in the provider network. The NetFlow Analyzer or the VPN solution center (VPN-SC) application collects this information and computes and displays site-to-site VPN traffic statistics.

Benefits to MPLS Egress NetFlow Accounting are as follows:

- Enhanced network monitoring for complete billing solution—You can now capture flows on the egress and ingress router interfaces to provide complete end-to-end usage information on network traffic. The accounting server uses the collected data for various levels of aggregation for accounting reports and API accounting information, thus providing a complete billing solution.
- More accurate accounting statistics—NetFlow data statistics now account for all the packets that are dropped in the core of the service provider network, thus providing more accurate traffic statistics and patterns.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring MPLS



Configuring Multiprotocol Label Switching

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes how to configure your network to perform Multiprotocol Label Switching (MPLS).

This chapter contains the following sections:

- [Configuring MPLS Levels of Control](#)
- [Configuring a Router for MPLS Forwarding](#)
- [Configuring MPLS Traffic Engineering](#)
- [Configuring MPLS Traffic Engineering Paths](#)
- [Configuring MPLS Virtual Private Networks](#)
- [Configuring MPLS QoS Backbone Support](#)
- [Configuring MPLS QoS](#)
- [Configuring the MPLS Label Switch Controller](#)
- [Configuring MPLS Egress NetFlow Accounting](#)
- [Verifying Configuration of MPLS Forwarding](#)

For configuration examples on MPLS, see the “[MPLS Configuration Examples](#)” section.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the section “[Identifying Supported Platforms](#)” in the chapter “Using Cisco IOS Software.”



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Configuring MPLS Levels of Control

This section describes three sample cases where MPLS is configured on Cisco 7500 and 7200 series routers. These cases show the levels of control possible in selecting how MPLS is deployed in a network.

[Table 1](#) lists the cases, including the steps to perform MPLS and their corresponding Cisco IOS CLI commands.

Table 1 *MPLS—Levels of Control*

Levels of Control Examples	Description
Case 1—Enable MPLS Incrementally in a Network	The steps necessary for incrementally deploying MPLS through a network, assuming that packets to all destination prefixes should be label switched.
Case 2—Route Labeled Packets to Network A Only	The mechanism by which MPLS can be restricted, such that packets are label switched to only a subset of destinations.
Case 3—Limit Label Distribution on an MPLS Network	The mechanisms for further controlling the distribution of labels within a network.

For more information about the Cisco IOS CLI commands, see the chapter “MPLS Commands” in the *Cisco IOS Switching Services Command Reference*.

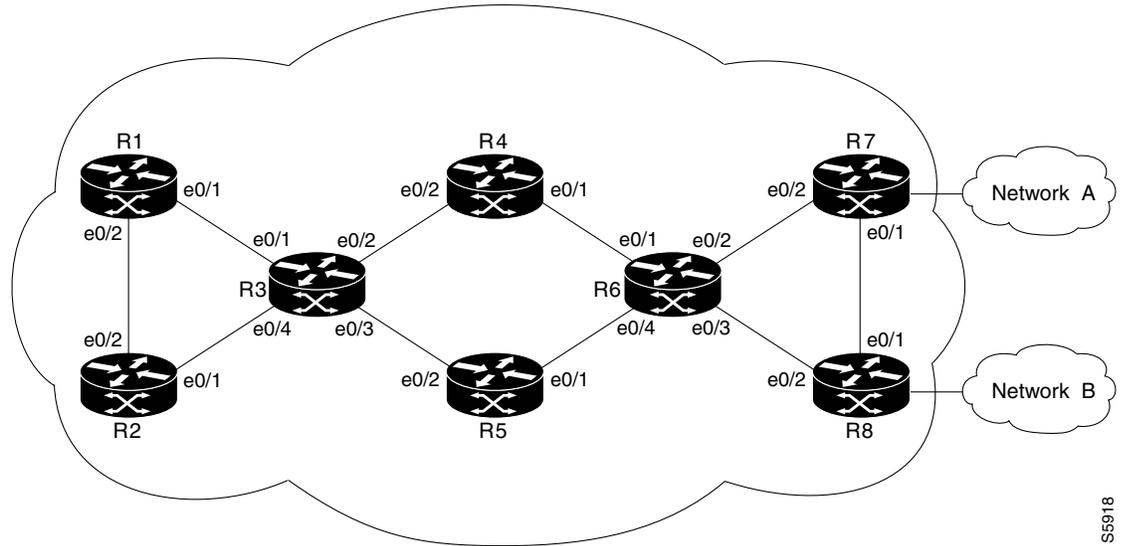
[Figure 1](#) shows a router-only MPLS network with Ethernet interfaces. The following sections outline the procedures for configuring MPLS and displaying MPLS information in a network based on the topology shown in [Figure 1](#).



Note

Ethernet interfaces are shown in [Figure 1](#), but any of the interfaces that are supported could be used instead. ATM interfaces operating as TC-ATM interfaces are the exception to this statement.

Figure 1 A Router-Only MPLS Network with Ethernet Interfaces



81693

Case 1—Enable MPLS Incrementally in a Network

In the first case, assume that you want to deploy MPLS incrementally throughout a network of routers, but that you do not want to restrict which destination prefixes are label switched. For a description of the commands listed in these cases, see the chapter “MPLS Commands” in the *Cisco IOS Switching Services Command Reference*.

To enable MPLS incrementally in a network, use the following commands beginning in router configuration mode (see [Figure 1](#)):

	Command	Purpose
Step 1	<pre> At R1: Router# configuration terminal Router(config)# ip cef distributed Router(config)# tag-switching advertise-tags Router(config)# interface e0/1 Router(config-if)# tag-switching ip Router(config-if)# exit At R3: Router# configuration terminal Router(config)# ip cef distributed Router(config)# tag-switching advertise-tags Router(config)# interface e0/1 Router(config-if)# tag-switching ip </pre>	<p>Enables MPLS between R1 and R3.</p> <p>In order to configure distributed VIP MPLS, you must configure dCEF switching. Enter the ip cef distributed global configuration command on all routers.</p>
Step 2	<pre> At R3: Router(config)# interface e0/2 Router(config-if)# tag-switching ip Router(config-if)# exit At R4: Router# configuration terminal Router(config)# ip cef distributed Router(config)# tag-switching advertise-tags Router(config)# interface e0/2 Router(config-if)# tag-switching ip Router(config-if)# exit </pre>	<p>Enables MPLS between R3 and R4.</p>

After you perform these steps, R1 applies labels to packets that are forwarded through Ethernet interface e0/1, with a next hop to R3.

You can enable MPLS throughout the rest of the network by repeating steps 1 and 2 as appropriate on other routers until all routers and interfaces are enabled for MPLS. See the example in the [“Enabling MPLS Incrementally in a Network Example”](#) section.

Case 2—Route Labeled Packets to Network A Only

In the second case, assume that you want to enable MPLS for a subset of destination prefixes. This option might be used to test MPLS across a large network. In this case, you would configure the system so that only a small number of destinations is label switched (for example, internal test networks) without the majority of traffic being affected.

To enable MPLS for a subset of destination prefixes, use the following commands at each router in the network in router configuration mode (see [Figure 1](#)):

	Command	Purpose
Step 1	Router(config)# access-list 1 permit A	Limits label distribution by using an access list. (Enter the actual network address and netmask in place of permit A. For example, access-list 1 permit 192.5.34.0 0.0.0.255.)
Step 2	Router(config)# tag-switching advertise-tags for 1	Instructs the router to advertise for network A only to all adjacent label switch routers. Any labels for other destination networks that the router may have distributed before this step are withdrawn.

Case 3—Limit Label Distribution on an MPLS Network

The third case demonstrates the full control available to you in determining the destination prefixes and paths for which MPLS is enabled.

Configure the routers so that packets addressed to network A are labeled, all other packets are unlabeled, and only links R1-R3, R3-R4, R4-R6, and R6-R7 carry labeled packets addressed to network A. For example, suppose the normally routed path for packets arriving at R1 addressed to network A or network B is R1, R3, R5, R6, R7. A packet addressed to network A would flow labeled on links R1-R3 and R6-R7, and unlabeled on links R3-R5 and R5-R6. A packet addressed to network B would follow the same path, but would be unlabeled on all links.

Assume that at the outset the routers are configured so that packets addressed to network A are labeled and all other packets are unlabeled (as at the completion of Case 2).

Use the **tag-switching advertise-tags** command and access lists to limit label distribution. Specifically, you need to configure routers R2, R5, and R8 to distribute no labels to other routers. This ensures that no other routers send labeled packets to any of those three. You also need to configure routers R1, R3, R4, R6, and R7 to distribute labels only for network A and to distribute them only to the appropriate adjacent router; that is, R3 distributes its label for network A only to R1, R4 only to R3, and so on.

To limit label distribution on a MPLS network, use the following commands in router configuration mode:

	Command	Purpose
Step 1	Router(config)# no tag-switching advertise-tags	Configures R2 to distribute no labels.
Step 2	Router(config)# no tag-switching advertise-tags	Configures R5 to distribute no labels.
Step 3	Router(config)# no tag-switching advertise-tags	Configures R8 to distribute no labels.

	Command	Purpose
Step 4	<pre>Router(config)# access-list 2 permit R1 Router(config)# no tag-switching advertise-tags for 1 Router(config)# tag-switching advertise-tags for 1 to 2 Router(config)# exit</pre>	<p>Configures R3 by defining an access list and by instructing the router to distribute labels for the networks permitted by access list 1 (created as part of case 2) to the routers permitted by access list 2.</p> <p>The access list 2 permit R1 command permits R1 and denies all other routers.</p> <p>(Enter the actual network address and netmask in place of permit R1. For example, access-list 1 permit 192.5.34.0 0.0.0.255.)</p>
Step 5	<pre>Router(config)# access-list 1 permit A Router(config)# access-list 2 permit R1 Router(config)# tag-switching advertise-tags for 1 to 2 Router(config)# exit</pre>	<p>Configures R3.</p> <p>(Enter the actual network address and netmask in place of permit R1. For example, access-list 1 permit 192.5.34.0 0.0.0.255.)</p>
Step 6	<pre>Router(config)# access-list 1 permit A Router(config)# access-list 2 permit R3 Router(config)# tag-switching advertise-tags for 1 to 2 Router(config)# exit</pre>	<p>Configures R4.</p> <p>(Enter the actual network address and netmask in place of permit R1. For example, access-list 1 permit 192.5.34.0 0.0.0.255.)</p>
Step 7	<pre>Router(config)# access-list 1 permit A Router(config)# access-list 2 permit R4 Router(config)# tag-switching advertise-tags for 1 to 2 Router(config)# exit</pre>	<p>Configures R6.</p> <p>(Enter the actual network address and netmask in place of permit R1. For example, access-list 1 permit 192.5.34.0 0.0.0.255.)</p>
Step 8	<pre>Router(config)# access-list 1 permit A Router(config)# access-list 2 permit R6 Router(config)# tag-switching advertise-tags for 1 to 2 Router(config)# exit</pre>	<p>Configures R7.</p> <p>(Enter the actual network address and netmask in place of permit R1. For example, access-list 1 permit 192.5.34.0 0.0.0.255.)</p>

Configuring a Router for MPLS Forwarding

MPLS forwarding on routers requires that CEF be enabled. To enable CEF on a router, enter the following commands:

```
Router# configure terminal
Router(config)# ip cef [distributed]
```



Note

For best MPLS forwarding performance, use the **distributed** option on routers that support this option.

For more information on the CEF commands, refer to the *Cisco IOS Switching Services Command Reference*.

Configuring MPLS Traffic Engineering

Perform the following tasks before you enable MPLS traffic engineering:

- Turn on MPLS tunnels
- Turn on CEF
- Turn on IS-IS or OSPF

To configure MPLS traffic engineering, perform the tasks described in the following sections:

- [Configuring a Device to Support Tunnels](#)
- [Configuring an Interface to Support RSVP-Based Tunnel Signalling and IGP Flooding](#)
- [Configuring IS-IS for MPLS Traffic Engineering](#)
- [Configuring OSPF for MPLS Traffic Engineering](#)
- [Configuring an MPLS Traffic Engineering Tunnel](#)

Configuring a Device to Support Tunnels

To configure a device to support tunnels, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip cef	Enables standard CEF operation. For information about CEF configuration and the command syntax, see the <i>Cisco IOS Switching Services Command Reference</i> .
Step 2	Router(config)# mpls traffic-eng tunnels	Enables the MPLS traffic engineering tunnel feature on a device.

Configuring an Interface to Support RSVP-Based Tunnel Signalling and IGP Flooding

To configure an interface to support RSVP-based tunnel signalling and IGP flooding, use the following commands in interface configuration mode:



Note

You must enable the tunnel feature on interfaces that you want to support MPLS traffic engineering.

	Command	Purpose
Step 1	Router(config-if)# mpls traffic-eng tunnels	Enables MPLS traffic engineering tunnels on an interface.
Step 2	Router(config-if)# ip rsvp bandwidth <i>bandwidth</i>	Enables RSVP for IP on an interface and specifies the amount of bandwidth that will be reserved. For a description of the ip rsvp interface command syntax, see the <i>Cisco IOS Quality of Service Solutions Command Reference</i> .

Configuring IS-IS for MPLS Traffic Engineering

To configure IS-IS for MPLS traffic engineering, perform the steps described below. For a description of the IS-IS commands (excluding the IS-IS traffic engineering commands), see the *Cisco IOS IP and IP Routing Command Reference*.

	Command	Purpose
Step 1	Router(config)# router isis	Enables IS-IS routing and specifies an IS-IS process for IP. This command places the router in router configuration mode.
Step 2	Router(config-router)# mpls traffic-eng level-1	Turns on MPLS traffic engineering for IS-IS level 1.
Step 3	Router(config-router)# mpls traffic-eng router-id loopback0	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0.
Step 4	Router(config-router)# metric-style wide	Configures a router to generate and accept only new-style TLVs.

Configuring OSPF for MPLS Traffic Engineering

To configure OSPF for MPLS traffic engineering, use the following commands beginning in global configuration mode. For a description of the OSPF commands (excluding the OSPF traffic engineering commands), see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

	Command	Purpose
Step 1	Router(config)# router ospf <i>process-id</i>	Configures an OSPF routing process for IP and places the router in configuration mode. The <i>process-id</i> argument is an internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process.
Step 2	Router(config-router)# mpls traffic-eng area 0	Turns on MPLS traffic engineering for OSPF area 0.
Step 3	Router(config-router)# mpls traffic-eng router-id loopback0	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0.

Configuring an MPLS Traffic Engineering Tunnel

To configure an MPLS traffic engineering tunnel, use the following commands in interface configuration mode. This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

	Command	Purpose
Step 1	Router(config)# interface tunnel	Configures an interface type and enters interface configuration mode.
Step 2	Router(config)# ip unnumbered loopback0	Gives the tunnel interface an IP address. An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.
Step 3	Router(config-if)# tunnel destination <i>A.B.C.D</i>	Specifies the destination for a tunnel.
Step 4	Router(config-if)# tunnel mode mpls traffic-eng	Sets the tunnel encapsulation mode to MPLS traffic engineering.
Step 5	Router(config-if)# tunnel mpls traffic-eng bandwidth <i>bandwidth</i>	Configures the bandwidth for the MPLS traffic engineering tunnel.
Step 6	Router(config-if)# tunnel mpls traffic-eng path-option <i>number</i> { dynamic explicit { <i>name path-name</i> <i>path-number</i> }} [lockdown]	Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database. A dynamic path is used if an explicit path is unavailable.

Configuring MPLS Traffic Engineering Paths

To configure an MPLS traffic engineering tunnel that an IGP can use, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# interface tunnel1	Configures an interface type and enters interface configuration mode.
Step 2	Router(config-if)# tunnel mpls traffic-eng autoroute announce	Causes the IGP to use the tunnel in its enhanced SPF calculation.

Configuring MPLS Virtual Private Networks

To configure and verify VPNs, perform the tasks described in the following sections:

- [Defining VPNs](#)
- [Configuring BGP Routing Sessions](#)
- [Configuring PE to PE Routing Sessions](#)
- [Configuring BGP PE to CE Routing Sessions](#)
- [Configuring RIP PE to CE Routing Sessions](#)
- [Configuring Static Route PE to CE Routing Sessions](#)

- [Configuring MPLS VPNs with Cable Interfaces](#)
- [Configuring Interautonomous Systems for MPLS VPNs](#)
- [Verifying VPN Operation](#)

Defining VPNs

To define VPN routing instances, use the following commands beginning in router configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# ip vrf <i>vrf-name</i>	Enters VRF configuration mode and defines the VPN routing instance by assigning a VRF name.
Step 2	Router(config-vrf)# rd <i>route-distinguisher</i>	Creates routing and forwarding tables.
Step 3	Router(config-vrf)# route-target { import export both } <i>route-target-ext-community</i>	Creates a list of import or export route target communities for the specified VRF.
Step 4	Router(config-vrf)# import map <i>route-map</i>	(Optional) Associates the specified route map with the VRF.
Step 5	Router(config-vrf)# export map <i>route-map</i>	(Optional) Associates the specified export route map with the VRF.
Step 6	Router(config-if)# ip vrf forwarding <i>vrf-name</i>	Associates a VRF with an interface or subinterface.

Configuring BGP Routing Sessions

To configure BGP routing sessions in a provider network, use the following commands beginning in router configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# router bgp <i>autonomous-system</i>	Configures the BGP routing process with the autonomous system number passed along to other BGP routers.
Step 2	Router(config-router)# neighbor { <i>ip-address</i> <i>peer-group-name</i> } remote-as <i>number</i>	Specifies a neighbor's IP address or BGP peer group identifying it to the local autonomous system.
Step 3	Router(config-router)# neighbor <i>ip-address</i> activate	Activates the advertisement of the IPv4 address family.

Configuring PE to PE Routing Sessions

To configure PE to PE routing sessions in a provider network, use the following commands beginning in router configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config-router)# address-family vpnv4 [unicast multicast]	Defines IBGP parameters for VPNv4 NLRI exchange.
Step 2	Router(config-router-af)# neighbor address remote-as as-number	Defines an IBGP session to exchange VPNv4 NLRI.
Step 3	Router(config-router-af)# neighbor address activate	Activates the advertisement of the IPv4 address family.

Configuring BGP PE to CE Routing Sessions

To configure BGP PE to CE routing sessions, use the following commands beginning in router configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config-router)# address-family ipv4 [unicast] vrf vrf-name	Defines EBGP parameters for PE to CE routing sessions. Note The default is Off for autosummary and synchronization in the VRF address-family submode.
Step 2	Router(config-router-af)# neighbor address remote-as as-number	Defines an EBGP session between PE and CE routers.
Step 3	Router(config-router-af)# neighbor address activate	Activates the advertisement of the IPv4 address family.

Configuring RIP PE to CE Routing Sessions

To configure RIP PE to CE routing sessions, use the following commands beginning in router configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# router rip	Enables RIP.
Step 2	Router(config-router-af)# address-family ipv4 [unicast] vrf vrf-name	Defines RIP parameters for PE to CE routing sessions. Note The default is Off for auto-summary and synchronization in the VRF address-family submode.
Step 3	Router(config-router-af)# network prefix	Enables RIP on the PE to CE link.

Configuring Static Route PE to CE Routing Sessions

To configure static route PE to CE routing sessions, use the following commands in router configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# ip route vrf vrf-name	Defines static route parameters for every PE to CE session.
Step 2	Router(config-router)# address-family ipv4 [unicast] vrf vrf-name	Defines static route parameters for every BGP PE to CE routing session. Note The default is Off for auto-summary and synchronization in the VRF address-family submode.
Step 3	Router(config-router-af)# redistribute static	Redistributes VRF static routes into the VRF BGP table.
Step 4	Router(config-router-af)# redistribute connected	Redistributes directly connected networks into the VRF BGP table.

Configuring MPLS VPNs with Cable Interfaces

Before configuring IP-based VPNs on Cisco uBR7200 series, perform the following tasks:

- Ensure that your network supports reliable broadband data transmission. Your network area must be swept, balanced, and certified based on National Television Standards Committee (NTSC) or appropriate international cable plant recommendations. Ensure that your network area meets all DOCSIS or European Data-over-Cable Service Interface Specifications (EuroDOCSIS) downstream and upstream RF requirements.
- Ensure that your Cisco uBR7200 series universal broadband router is installed following instructions in the *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* and the *Regulatory Compliance and Safety Information for the Cisco uBR7200 Series Universal Broadband Router*.
- Ensure that your Cisco uBR7200 series universal broadband router is configured for basic operations following instructions in the *Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide*. The chassis must contain at least one port adapter to provide backbone connectivity and one Cisco cable modem card to serve as the RF cable TV interface.

To configure MPLS VPNs with cable interfaces, perform the tasks described in the following sections. The first two sections are required tasks; the remaining tasks are optional:

- [Creating VRFs for Each VPN](#) (Required)
- [Defining Subinterfaces on a Physical Cable Interface and Assigning VRFs](#) (Required)
- [Configuring Cable Interface Bundles](#) (Optional)
- [Configuring Subinterfaces and MPLS VPNs on a Bundle Master](#) (Optional)
- [Configuring MPLS in the P Routers in the Provider Core](#) (Optional)
- [Verifying the MPLS VPN Configuration](#) (Optional)

Restrictions

The following restrictions apply to configuring MPLS VPNs with cable interfaces:

- Each subinterface on the CMTS requires an address range from the ISP and from the MSO. These two ranges must not overlap and must be extensible to support an increased number of subscribers for scalability. Cisco IOS Release 12.1(2)EC and 12.1(2)T do not support overlapping addresses for the MPLS VPN subinterface.



Note This document does not address allocation and management of MSO and ISP IP addresses. See *Configuring Multiprotocol Label Switching* for this information.

- Cisco IOS Release 12.1(2) T supports the **cable source-verify dhcp** cable interface command, but Cisco IOS Release 12.1(2)EC does not support it. The **cable source-verify dhcp** cable interface command enables Dynamic Host Control Protocol (DHCP) servers to verify IP addresses of upstream traffic, and prevent MSO users from using unauthorized, spoofed, or stolen IP addresses.
- When using only MPLS VPNs, create subinterfaces on the bundle master, assign them an IP address, and provide VRF configuration for each ISP. When you create subinterfaces and configure only MPLS VPNs, the cable interface bundling feature is independent of the MPLS VPN.
- When using cable interface bundling, perform the following tasks:
 - Define one of the interfaces in the bundle as the bundle master interface.
 - Specify all generic IP networking information (such as IP address, routing protocols, and switching modes) on the bundle master interface. Do not specify generic IP networking information on bundle slave interfaces. If you attempt to add an interface to a bundle as a nonmaster interface and an IP address is assigned to this interface, the command will fail. You must remove the IP address configuration before you can add the interface to a bundle.
 - An interface that has a subinterfaces defined over it is not allowed to be a part of the bundle.
 - Specify generic (not downstream or upstream related) cable interface configurations, such as source-verify or ARP handling, on the master interface. Do not specify generic configuration on nonmaster interfaces.
 - If you configure an interface as a part of a bundle and it is not the master interface, all generic cable configuration for this interface is removed. The master interface configuration will then apply to all interfaces in the bundle.
- Cable interface bundling is only supported on cable interfaces. Cisco IOS software provides cable interfaces with Cisco uBR-MC11, Cisco uBR-MC12, Cisco uBR-MC14, and Cisco uBR-MC16 cable modem cards.
- Interface bundles can only be configured using the command-line interface (including the CLI-based HTML configuration).

Creating VRFs for Each VPN

To create VRFs for each VPN, use the following commands beginning in router configuration mode:

**Note**

Because only the CMTS has logical subinterfaces, assignments of VRFs on the other PE devices will be to specific physical interfaces.

	Command	Purpose
Step 1	Router(config)# ip vrf <i>mgmt-vpn</i>	Enters VRF configuration mode and maps a VRF table to the VPN (specified by <i>mgmt-vpn</i> argument). The management VPN is the first VPN configured.
Step 2	Router(config-vrf)# rd <i>mgmt-rd</i>	Creates a routing and forwarding table by assigning a RD to the management VPN.
Step 3	Router(config-vrf)# route-target { export import both } <i>mgmt-rd</i>	Exports or imports all routes for the RD of the management VPN. This determines which routes will be shared within VRFs.
Step 4	Router(config-vrf)# route-target import <i>isp1-vpn-rd</i>	Imports all routes for the VPNs (<i>isp1-vpn</i> argument) route distinguisher.
Step 5	Router(config-vrf)# route-target import <i>isp2-vpn-rd</i>	Imports all routes for the VPNs (<i>isp2-vpn</i> argument) RD.
Step 6	Router(config-vrf)# ip vrf <i>isp1-vpn</i>	Creates a routing and forwarding table by assigning a RD to <i>isp1-vpn</i> argument) .
Step 7	Router(config-vrf)# rd <i>mgmt-rd</i>	Creates a routing and forwarding table by assigning a RD (<i>mgmt-rd</i> argument) to the management VPN (<i>mgmt-vpn</i> argument) .
Step 8	Router(config-vrf)# route-target export <i>isp1-vpn-rd</i>	Exports all routes for the VPNs (<i>isp1-vpn</i> argument) RD.
Step 9	Router(config-vrf)# route-target import <i>isp1-vpn-rd</i>	Imports all routes for the VPNs (<i>isp1-vpn</i> argument) RD.
Step 10	Router(config-vrf)# route-target import <i>mgmt-vpn-rd</i>	Exports all routes for the VPNs (<i>mgmt-vpn</i> argument) RD.
Step 11	Router(config-vrf)# ip vrf <i>isp2-vpn</i>	Creates a routing and forwarding table by assigning a RD to <i>isp2-vpn</i> argument) .
Step 12	Router(config-vrf)# route-target export <i>isp2-vpn-rd</i>	Exports all routes for the VPNs (<i>isp2-vpn</i> argument) RD.
Step 13	Router(config-vrf)# route-target import <i>isp2-vpn-rd</i>	Imports all routes for the VPNs (<i>isp2-vpn</i> argument) RD.
Step 14	Router(config-vrf)# route-target import <i>mgmt-vpn-rd</i>	Imports all routes for the VPNs (<i>mgmt-vpn</i> argument) RD.

Defining Subinterfaces on a Physical Cable Interface and Assigning VRFs

To create a logical cable subinterface, use the following commands beginning in global configuration mode. Create one subinterface for each VPN (one per ISP). The first subinterface created must be configured as part of the management VPN (with the lowest subinterface number). Create VRFs using the procedure described in the “Creating VRFs for Each VPN” section and apply them to the subinterface.

	Command	Purpose
Step 1	Router# configure terminal	Enters configuration mode.
Step 2	Router(config)# interface cable <i>slot/port</i>	Enters cable interface configuration mode. <i>slot</i> = slot number in chassis (slot numbers begin with a 0). <i>port</i> = port number on cable modem card slot (port numbers begin with a 0).
Step 3	Router(config-if)# interface cable <i>slot/port.n</i>	Defines the first (management) subinterface with the lowest subinterface number. Valid range for <i>n</i> is from 1 to 255.
Step 4	Router(config-subif)# description <i>string</i>	Identifies the subinterface as the management subinterface.
Step 5	Router(config-subif)# ip vrf forwarding <i>mgmt-vpn</i>	Assigns the subinterface to the management VPN (the MPLS VPN used by the MSO to supply service to customers).
Step 6	Router(config-subif)# ip address <i>ipaddress mask</i>	Assigns the subinterface an IP address and a subnet mask.
Step 7	Router(config-subif)# cable helper-address <i>ip-address cable-modem</i>	Forwards DHCP requests from cable modems to the IP address listed.
Step 8	Router(config-subif)# cable helper-address <i>ip-address host</i>	Forwards DHCP requests from hosts to the IP address listed.
Step 9	Router(config-if)# interface cable <i>slot/port.n</i>	Defines an additional subinterface for the ISP (such as <i>isp1</i>). Valid range for <i>n</i> is 1 to 255.
Step 10	Router(config-subif)# description <i>string</i>	Identifies the subinterface (such as subinterface for the <i>isp1-vpn</i> argument).
Step 11	Router(config-subif)# ip vrf forwarding <i>isp1-vpn</i>	Assigns the subinterface to <i>isp1-vpn</i> VPN.
Step 12	Router(config-subif)# ip address <i>ipaddress mask</i>	Assigns the subinterface an IP address and a subnet mask.
Step 13	Router(config-subif)# cable helper-address <i>ip-address cable-modem</i>	Forwards DHCP requests from cable modems to the IP address listed.
Step 14	Router(config-subif)# cable helper-address <i>ip-address host</i>	Forwards DHCP requests from hosts to the IP address listed.
Step 15	Router(config-if)# interface cable <i>slot/port.n</i>	Defines an additional subinterface for the ISP (such as <i>isp2</i>). Valid range for <i>n</i> is 1 to 255.
Step 16	Router(config-subif)# description <i>string</i>	Identifies the subinterface (such as subinterface for the <i>isp2-vpn</i> argument) .
Step 17	Router(config-subif)# ip vrf forwarding <i>isp2-vpn</i>	Assigns the subinterface to <i>isp2-vpn</i> VPN.

	Command	Purpose
Step 18	Router(config-subif)# ip address <i>ipaddress mask</i>	Assigns the subinterface an IP address and a subnet mask.
Step 19	Router(config-subif)# cable helper-address <i>ip-address cable-modem</i>	Forwards DHCP requests from cable modems to the IP address listed.
Step 20	Router(config-subif)# cable helper-address <i>ip-address host</i>	Forwards DHCP requests from hosts to the IP address listed.
Step 21	Router(config)# copy running-config startup-config	Returns to configuration mode, and stores the configuration or changes to your startup configuration in NVRAM.
		 <p>Note Use this command to save the configuration settings that you created in the Cisco uBR7200 series universal broadband router using the configuration mode, the setup facility, and AutoInstall. If you fail to do this, your configuration will be lost the next time you reload the router.</p>
Step 22	Router(config)# exit	Returns to configuration mode.

Configuring Cable Interface Bundles

To assign a cable interface to a bundle, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface cable <i>slot/port</i>	Enters the cable interface configuration mode. <i>slot</i> = slot number in chassis (slot numbers begin with 0). <i>port</i> = port number on cable modem card slot (port numbers begin with 0). IP addresses are not assigned to this interface. They are assigned to the logical subinterfaces created within this interface.
Step 2	Router(config-if)# cable bundle <i>bundle-number master</i>	Defines the interface as the bundle's master interface. Valid range for <i>bundle-number</i> argument is from 1 to 255.

	Command	Purpose
Step 3	Router(config)# interface cable <i>slot/port</i>	Enters the cable interface configuration mode for another cable interface. <i>slot</i> = slot number in chassis (slot numbers begin with 0). <i>port</i> = port number on cable modem card slot (port numbers begin with 0). IP addresses are not assigned to this interface. They are assigned to the logical subinterfaces created within this interface.
Step 4	Router(config-if)# cable bundle <i>bundle-number</i>	Adds the interface to the bundle specified by <i>bundle-number</i> . Valid range for the <i>bundle-number</i> argument is from 1 to 255.

Configuring Subinterfaces and MPLS VPNs on a Bundle Master

To configure subinterfaces on a bundle master and assign each subinterface a Layer 3 configuration, configure cable interface bundles using the procedure described in the “[Configuring Cable Interface Bundles](#)” section.

Define subinterfaces on the bundle master interface and assign a Layer 3 configuration to each subinterface using the procedure described in the “[Defining Subinterfaces on a Physical Cable Interface and Assigning VRFs](#)” section. Create one subinterface for each customer VPN (one per ISP).

Configuring MPLS in the P Routers in the Provider Core

To configure MPLS in the P routers in the provider core, use the following commands beginning in router configuration mode:

	Command	Purpose
Step 1	Router(config)# ip cef	Enables CEF operation.
Step 2	Router(config)# interface FastEthernet <i>slot/port</i>	Enters FastEthernet interface configuration mode.
Step 3	Router(config-if)# ip address <i>ip-address mask</i>	Defines the primary IP address range for the interface.
Step 4	Router(config-if)# mpls ip	Enables the interface to be forwarded to an MPLS packet.
Step 5	Router(config-if)# mpls label-protocol ldp	Enables Label Distribution Protocol (LDP) on the interface.

	Command	Purpose
Step 6	Router(config)# copy running-config startup-config	Stores the configuration or changes to your startup configuration in NVRAM.  Note Use this command to save the configuration settings that you created in the Cisco uBR7200 series universal broadband router using the configuration mode, the setup facility, and AutoInstall. If you fail to do this, your configuration will be lost the next time you reload the router.
Step 7	Router(config)# exit	Returns to the configuration mode.

Verifying the MPLS VPN Configuration

To verify MPLS VPN operations on PE routers, use the following EXEC commands:

	Command	Purpose
Step 1	Router# show ip vrf	Displays the set of VRFs and interfaces.
Step 2	Router# show ip route vrf	Displays the IP routing table for a VRF.
Step 3	Router# show ip protocols vrf	Displays the routing protocol information for a VRF.
Step 4	Router(config)# show cable bundle n forwarding-table	Displays the forwarding table for the specified interface.

Configuring Interautonomous Systems for MPLS VPNs

Before you configure EBGp routing between autonomous systems or subautonomous systems in an MPLS VPN, ensure that you have properly configured all MPLS VPN routing instances and sessions. The configuration tasks outlined in this section build from those configuration tasks.

Perform the following tasks before you enable configure EBGp routing between autonomous systems or subautonomous systems in an MPLS VPN:

- Define VPN routing instances
- Configure BGP routing sessions in the service provider (P) network
- Configure PE to PE routing sessions in the service provider (P) network
- Configure BGP PE to CE routing sessions

To configure the exchange of VPN-IPv4 addresses between two or more autonomous systems or subautonomous systems in a confederation, perform the tasks described in the following sections. The tasks in the following sections are described as required or optional:

- [Configuring EBGp Routing for the Exchange of VPN Routes Between Autonomous Systems \(Required\)](#)
- [Configuring EBGp Routing for the Exchange of VPN Routes Between Subautonomous Systems in a Confederation \(Required\)](#)
- [Displaying VPN-IPv4 LFIB Entries \(Optional\)](#)

Configuring EBGP Routing for the Exchange of VPN Routes Between Autonomous Systems

To configure an EBGP border edge router in an autonomous system to exchange VPN routes with another autonomous system, use the following commands beginning in global configuration mode:



Note

Enter the **redistribute connected subnets** command in the IGP configuration portion of the router to propagates host routes for VPN-IPv4 EBGP neighbors to other routers and provider edge routers. Alternatively, you can specify the next-hop-self address when you configure IBGP neighbors.

	Command	Purpose
Step 1	Router(config)# router bgp <i>autonomous-system</i>	Creates an EBGP routing process and assigns it an AS number. The autonomous system number is passed along to identify the router to EBGP routers in another autonomous system.
Step 2	Router(config)# no bgp default route-target filter	Disables BGP route-target filtering. All received BGP VPN-IPv4 routes are accepted by the router.
Step 3	Router(config-router)# address-family vpnv4 [<i>unicast</i>]	Configures a routing session to carry VPN-IPv4 addresses across the VPN backbone. Each address has been made globally unique by the addition of an 8-byte RD. Unicast is optional; use it if you need to specify a unicast prefix.
Step 4	Router(config-router-af)# neighbor <i>peer-group-name</i> remote-as <i>autonomous-system</i>	Enters the address-family submode and specifies a neighboring EBGP peer group. This EBGP peer group is identified to the specified autonomous system.
Step 5	Router(config-router-af)# neighbor <i>peer-group-name</i> activate	Activates the advertisement of the VPN-IPv4 address family to a neighboring EBGP router.
Step 6	Router(config-router-af)# exit-address-family	Exits from the address-family submode of the global configuration mode.

Configuring EBGP Routing for the Exchange of VPN Routes Between Subautonomous Systems in a Confederation

In this confederation, subautonomous system IGP domains must know the addresses of CEBGP-1 and CEBGP-2. If you do not specify a next-hop-self address as part of the router configuration, ensure that the addresses of all PE routers in the subautonomous system are distributed throughout the network, not just the addresses of CEBGP-1 and CEBGP-2.



Note

To ensure that the host routes for VPN-IPv4 EBGP neighbors are propagated (by means of the IGP) to the other routers and provider edge routers, specify the **redistribute connected** router configuration command in the IGP configuration portion of the CEBGP router. If you are using OSPF, make sure that the OSPF process is not enabled on the CEBGP interface where the “redistribute connected” subnet exists.

To configure EBGP border edge router in a confederation to exchange VPN routes with another subautonomous system, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# router bgp <i>subautonomous-system</i>	Creates an EBGp routing process and assigns it an autonomous system number. The subautonomous system number is passed along to identify the router to EBGp routers in other subautonomous systems.
Step 2	Router(config)# bgp confederation identifier <i>autonomous-system</i>	Defines an EBGp confederation by specifying a confederation identifier associated with each subautonomous system. The subautonomous systems appear as a single autonomous system.
Step 3	Router(config)# bgp confederation peers <i>subautonomous-systems</i>	Specifies the subautonomous systems that belong to the confederation (identifying neighbors from other subautonomous systems within the confederation as special EBGp peers).
Step 4	Router(config)# no bgp default route-target filter	Disables BGP route-target community filtering. All received BGP VPN-IPv4 routes are accepted by the router.
Step 5	Router(config-router)# address-family vpnv4 [<i>unicast</i>]	Configures a routing session to carry VPN-IPv4 addresses across the VPN backbone. Each address has been made globally unique by the addition of an 8-byte RD. Unicast is optional; use it if you need to specify a unicast prefix.
Step 6	Router(config-router-af)# neighbor peer-group-name remote-as <i>autonomous-system</i>	Enters the address-family submode and specifies a neighboring EBGp peer group. This EBGp peer group is identified to the specified subautonomous system.
Step 7	Router(config-router-af)# neighbor peer-group-name next-hop-self	Advertises the router as the next hop for the specified neighbor. If you specify a next-hop-self address as part of the router configuration, you need not use the redistribute connected router configuration command
Step 8	Router(config-router-af)# neighbor peer-group-name activate	Activates the advertisement of the VPN-IPv4 address family to a neighboring PE router in the specified subautonomous system.
Step 9	Router(config-router-af)# exit-address-family	Exits from the address-family submode of the global configuration mode.

Displaying VPN-IPv4 LFIB Entries

To display the VPN-IPv4 Label Forwarding Information Base (LFIB) entries at the border edge routers in the autonomous systems, use the following EXEC commands:

	Command	Purpose
Step 1	Router# show ip bgp vpnv4 all [<i>tags</i>]	Displays information about all VPN-IPv4 labels.
Step 2	Router# show tag-switching forwarding-table	Displays the contents of the LFIB (such as VPN-IPv4 prefix or length and BGP next hop destination for the route).

The following is an example of how the VPN-IPv4 LFIB entries appear when you use the **show tag-switching forwarding-table** privileged EXEC command:

```
Router# show tag-switching forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes switched	tag	Outgoing interface	Next Hop
33	33	10.120.4.0/24	0		Hs0/0	point2point
35	27	100:12:10.200.0.1/32 \	0		Hs0/0	point2point

**Note**

In this example, the Prefix field appears as a VPN-IPv4 RD, plus the prefix. If the value is longer than the Prefix column (as illustrated in the last line of the example), the output automatically wraps onto the next line in the forwarding table to preserve column alignment.

Verifying VPN Operation

To verify VPN operation by displaying routing information on the PE routers, use the following **show** commands, as needed:

Command	Purpose
Router# show ip vrf	Displays the set of defined VRFs and interfaces.
Router# show ip vrf [{ brief detail interfaces }] <i>vrf-name</i>	Displays information about defined VRFs and associated interfaces.
Router# show ip route vrf <i>vrf-name</i>	Displays the IP routing table for a VRF.
Router# show ip protocols vrf <i>vrf-name</i>	Displays the routing protocol information for a VRF.
Router# show ip cef vrf <i>vrf-name</i>	Displays the CEF forwarding table associated with a VRF.
Router# show ip interface <i>interface-number</i>	Displays the VRF table associated with an interface.
Router# show ip bgp vpnv4 all [tags]	Displays information about all BGP VPN-IPv4 prefixes.
Router# show tag-switching forwarding vrf <i>vrf-name</i> [<i>prefix mask/length</i>] [detail]	Displays label forwarding entries that correspond to VRF routes advertised by this router.

Configuring MPLS QoS Backbone Support

Several different methods exist for supporting QoS across an MPLS backbone, the choice depending on whether the core has label switch routers (LSRs) or ATM-LSRs. In each case, however, the QoS building blocks are the same: CAR, WRED, and WFQ.

Three configurations are described in this section:

- LSRs used at the core of the network backbone
- ATM-LSRs used at the core of the network backbone
- ATM switches without the MPLS feature enabled

LSRs

LSRs at the core of the MPLS backbone are usually either Cisco 7200 and Cisco 7500 series routers running MPLS software. Packets are processed as follows:

1. IP packets enter into the edge of the MPLS network.
2. The edge LSRs invoke CAR to classify the IP packets and possibly set IP precedence. Alternatively, IP packets can be received with their IP precedence already set.
3. For each packet, the router performs a lookup on the IP address to determine the next hop LSR.
4. The appropriate label is placed on the packet with the IP Precedence bits copied into every label entry in the MPLS header.
5. The labeled packet is then forwarded to the appropriate output interface for processing.
6. The packets are differentiated by class. This is done according to drop probability (WRED) or according to bandwidth and delay (WFQ). In either case, LSRs enforce the defined differentiation by continuing to employ WRED or WFQ on each hop.

ATM-LSRs

ATM-LSRs at the core implement the multiple label virtual circuit model (LVC). In the multiple LVC model, one label is assigned for each service class for each destination. The operation of the edge LSR is the same as that described previously for the LSR case, except that the output is an ATM interface. WRED is used to define service classes and determine discard policy during congestion.

In the multiple LVC model, however, class-based WFQ (CBWFQ) is used to define the amount of bandwidth available to each service class. Packets are scheduled by class during congestion. The ATM-LSRs participate in the differentiation of classes with WFQ and intelligently drop packets when congestion occurs. The mechanism for this discard activity is weighted early packet discard (WEPD).

ATM Switches

When the core network uses ATM switches and the edge of the network uses MPLS-enabled edge LSRs, the edge LSRs are interconnected through a mesh of ATM Forum PVCs (CBR, VBR, or UBR) over the ATM core switches. The edge LSRs invoke WFQ on a per-VC basis to provide differentiation based on the delay of each MPLS QoS multiplexed onto the ATM Forum PVC. Optionally, WRED can also be used on a per-VC basis to manage drop priority between classes when congestion occurs on the edge LSR.

Table 2 lists the MPLS QoS features supported on packet interfaces.

Table 2 *MPLS QoS Features Supported on Packet Interfaces*

MPLS QoS Packet Feature	Cisco 7500 Series	Cisco 7200 Series	Cisco 4000 Series	Cisco 3600 Series	Cisco 2600 Series
Per-interface WRED	X	X	X	X	Untested
Per-interface, per-flow WFQ	X	X	X	X	Untested
Per-interface, per-class WFQ	X	X	X	X	Untested

Table 3 lists the MPLS QoS features supported on ATM interfaces.

Table 3 *MPLS QoS Features Supported on ATM Interfaces*

MPLS QoS ATM Forum PVCs Feature	Cisco 7500 Series	Cisco 7200 Series	Cisco 4000 Series	Cisco 3600 Series	Cisco 2600 Series
Per-VC WRED	X ¹	X ¹	—	—	—
Per-VC WRED and per VC, per-class WFQ	—	X ¹	—	—	—
MPLS QoS Multi-VC or LBR Feature					
Per-interface WRED	X ²	X ²	—	—	—
Per-interface, per-class WFQ	X ²	X ²	—	—	—

1. This feature is only available on the PA-A3.
2. This feature is only available on the PA-A1.

Table 4 lists the MPLS QoS features supported on ATM switches.

Table 4 *MPLS QoS Features Supported on ATM Switches*

MPLS QoS ATM Forum PVCs Feature	BPX 8650 Series	MGX 8800 Series	LightStream 1010 ATM Switch ¹	Catalyst 8540 MSR ¹
MPLS QoS ATM Forum PVCs	X	X	X	X
MPLS QoS Multi-VC or LBR—per-class WFQ	X	—	—	—

1. This switch can be used for the core only.

Configuring MPLS QoS

Perform the following tasks before you enable MPLS traffic engineering:

- Turn on MPLS tunnels
- Turn on CEF

To configure MPLS QoS, perform the tasks described in the following sections. The first five sections are described as required; the remaining tasks are optional:

- [Configuring QoS](#) (Required)
- [Setting the MPLS Experimental Field Value](#) (Required)
- [Using the Modular QoS CLI to Configure the Ingress Label Switching Router](#) (Required)
- [Using CAR to Configure the Ingress Label Switching Router](#) (Required)
- [Configuring the Output IP QoS of the Packet](#) (Required)
- [Configuring PVC Mode in a Non-MPLS-Enabled Core](#) (Optional)

- [Configuring Multi-VC Mode in a MPLS-Enabled Core \(Optional\)](#)
- [Configuring Multi-VCs Using the Cos-Map Function \(Optional\)](#)
- [Configuring DWFQ and Changing Queue Weights on an Outgoing Interface \(Optional\)](#)
- [Verifying QoS Operation \(Optional\)](#)

Configuring QoS

To configure QoS, you can configure one or more of the following features (in addition, of course, to other items not described in this document):

- CAR
- WRED
- WFQ

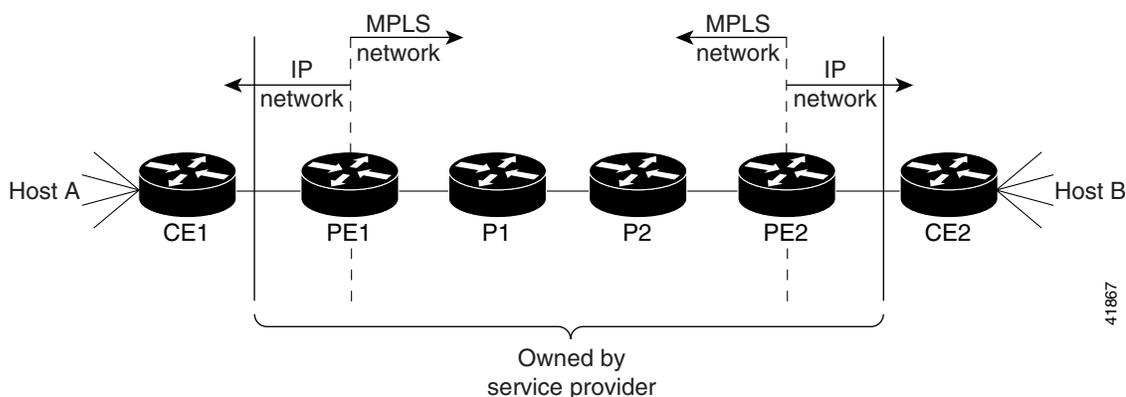
Setting the MPLS Experimental Field Value

Setting the MPLS experimental field value satisfies the requirement of service providers that do not want the value of the IP Precedence field modified within IP packets transported through their networks.

By choosing different values for the MPLS experimental field, you can mark packets based on their characteristics, such as rate or type, so that packets have the priority that they require during periods of congestion.

[Figure 2](#) shows a MPLS network of a service provider that connects two sites of a network belonging to a customer.

Figure 2 *MPLS Network Connecting Two Sites of a Customer's IP Network*



To use these features in a network, set the MPLS experimental field value at PE1 (the ingress label switching router) by using the modular QoS CLI or the **rate-limit** interface command that CAR provides to set the QoS value in the MPLS packet. For detailed instructions, see the [“Setting the MPLS Experimental Field Value”](#) section.

Importance of Prioritizing a Packet Appropriately

During Step 1 of the configuration process (described in the “Using the Modular QoS CLI to Configure the Ingress Label Switching Router” and “Using CAR to Configure the Ingress Label Switching Router” sections) you classify IP packets according to their source address, destination address, port, protocol identification, or quality of service field. For example, packets can be identified based on one or more of the specified fields, as Voice over IP (VoIP) or a File Transfer Protocol (FTP). Packet classification/marketing is important because a priority of a packet is determined by how it is classified or marked.

A priority of a packet affects how the packet is treated during periods of congestion. For example, service providers have service level agreements (SLAs) with customers. The agreement specifies how much traffic the service provider has agreed to deliver. To comply with the agreement, the customer must not send more than the agreed-upon rate. Packets are considered to be in-rate or out-of-rate. If there is congestion in the network, out-of-rate packets might be dropped more aggressively.

Configuring the Ingress MPLS Router

To classify IP packets, you configure the ingress label switching router. Packets are received at the ingress router as IP packets and sent as MPLS packets. To perform the configuration, use either of the following features:

- Modular QoS CLI, the newer and more flexible method—Use this method if you do not want to consider the rate of the packets that PE1 receives.
- CAR—Use if you want to consider the rate of the incoming packets:
 - If a packet conforms to the SLA between the service provider and the customer (that is, the packet is in-rate), the service provider gives the packet preferential treatment when the network of a service provider is congested.
 - If a packet does not conform (that is, it is out-of-rate) and the network is congested, the service provider might discard the packet or give it less preferential treatment.

Using the Modular QoS CLI to Configure the Ingress Label Switching Router

To use the modular QoS CLI to configure PE1 (the ingress label switching router), perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Configure a class map to classify IP packets according to their IP precedence. |
| Step 2 | Configure a policy map to mark MPLS packets. (Write their classification into the MPLS experimental field.) |
| Step 3 | Configure the input interface to attach the service policy. |
-

Configuring a Class Map to Classify IP Packets

To configure a class map, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# class-map <i>class-map name</i>	Specifies the class map to which packets will be matched.
Step 2	Router(config-c-map)# match <i>criteria</i>	Specifies the packet characteristics that will be matched to the class.
Step 3	Router(config-c-map)# end	Exits class-map configuration mode.

In the following example, all packets that contain IP Precedence 4 are matched by the class-map name IP_prec4:

```
Router(config)# class-map IP_prec4
Router(config-c-map)# match ip precedence 4
Router(config-c-map)# end
```

Configuring a Policy Map to Set the MPLS Experimental Field

To configure a policy map, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# policy-map <i>policy-map name</i>	Creates a policy map that can be attached to one or more interfaces to specify a service policy.
Step 2	Router(config-p-map)# class <i>class-map name</i>	Specifies the name of the class map previously designated in the class-map command.
Step 3	Router(config-p-map-c)# set mpls experimental <i>value</i>	Designates the value to which the MPLS bits are set if the packets match the specified policy map.
Step 4	Router(config-p-map-c)# end	Exits policy-map configuration mode.

In the following example, the value in the MPLS experimental field of each packet that is matched by the class-map IP_prec4 is set to 5:

```
Router(config)# policy-map set_experimental_5
Router(config-p-map)# class IP_prec4
Router(config-p-map-c)# set mpls experimental 5
Router(config-p-map-c)# end
```

Configuring the Input Interface to Attach the Service Policy

To configure the input interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface <i>name</i>	Designates the input interface.
Step 2	Router(config-int)# service-policy input <i>policy-map name</i>	Attaches the specified policy map to the input interface.
Step 3	Router(config-int)# end	Exits interface configuration mode.

In the following example, the service policy `set_experimental_5` is attached to an Ethernet input interface:

```
Router(config)# interface ethernet 1/0/0
Router(config-int)# service-policy input set_experimental_5
Router(config-int)# end
```

Using CAR to Configure the Ingress Label Switching Router

To use CAR to configure the ingress label switching router, perform the following steps:

-
- Step 1** Configure an IP rate-limit access list for classifying IP packets according to their IP precedence. Perform this step at PE1 (the ingress LSR).
 - Step 2** Configure a rate limit on an input interface to set MPLS packets. (Write the classification of the packet into the MPLS experimental field.)
-

These steps are explained in the following sections.

Configuring a Rate Limit Access List for Classifying IP Packets

To configure a rate limit access list, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# access-list rate-limit <i>acl-index</i> <i>precedence</i>	Specifies the criteria to be matched.
Step 2	Router(config)# end	Exits configuration mode.

In the following example, all packets that contain IP Precedence 4 are matched by the rate-limit access list 24:

```
Router(config)# access-list rate-limit 24 4
Router(config)# end
```

Configuring a Rate-Limit on an Input Interface to Set MPLS Packets

To configure a rate-limit on an input interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface <i>name</i>	Designates the input interface.
Step 2	Router(config-int)# rate-limit input [access-group [rate-limit] <i>acl-index</i>] <i>bps burst-normal burst-max conform-action set-mpls-exp-transmit exp exceed-action set-mpls-exp-transmit exp</i>	Specifies the action to take on packets during label imposition.

In the following example, the experimental field for the output MPLS packet is set to 4 if the input IP packets match the access list and conform to the rate. The MPLS experimental field is set to 0 if packets match access list 24 and exceed the input rate.

```
Router(config)# interface ethernet 1/0/0
Router(config-int)# rate-limit input access-group rate-limit 24 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
```

Configuring the Output IP QoS of the Packet

The output QoS of the packet is determined by the IP header information. For configuration details, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Configuring PVC Mode in a Non-MPLS-Enabled Core

To configure a PVC in a non-MPLS-enabled core, use the following commands beginning in router configuration mode:

	Command	Purpose
Step 1	Router(config)# interface type number point-to-point	Configures a point-to-point ATM subinterface.
Step 2	Router(config-subif)# ip unnumbered Loopback0	Assigns an IP address to the subinterface.
Step 3	Router(config-subif)# pvc 4/40	Creates a PVC on the subinterface.
Step 4	Router(config-if-atm-vc)# random-detect attach groupname	Activates WRED or dWRED on the interface.
Step 5	Router(config-if-atm-vc)# encapsulation aal5snap	Sets encapsulation type for the PVC.
Step 6	Router(config-subif)# exit	Exits from PVC mode and enters subinterface mode.
Step 7	Router(config-subif)# tag-switching ip	Enables MPLS IP on the point-to-point interface.

Configuring Multi-VC Mode in a MPLS-Enabled Core

To configure multi-VC mode in an MPLS-enabled core, use the following commands beginning in router configuration mode:



Note

The default for the multi-VC mode creates four VCs for each MPLS destination.

	Command	Purpose
Step 1	Router(config)# interface type number tag-switching	Configures an ATM MPLS subinterface.
Step 2	Router(config-subif)# ip unnumbered Loopback0	Assigns an IP address to the subinterface.
Step 3	Router(config-subif)# tag-switching atm multi-vc	Enables ATM multi-VC mode on the subinterface.
Step 4	Router(config-subif)# tag-switching ip	Enables MPLS on the ATM subinterface.

Configuring Multi-VCs Using the Cos-Map Function

If you do not choose to use the default for configuring label VCs, you can configure fewer label VCs by using the QoS map function. To use the QoS map function, use the following commands beginning in router configuration mode:

	Command	Purpose
Step 1	Router(config)# tag-switching cos-map <i>cos-map number</i>	Creates a QoS map.
Step 2	Router(config-tag-cos-map) # class 1 premium	Enters the cos-map submodule and maps premium and standard classes to label VCs. This QoS map assigns class 1 traffic to share the same label VC as class 2 traffic. The numbers you assign to the QoS map range from 0 to 3. The defaults are: <ul style="list-style-type: none"> • class 0 is available • class 1 is standard • class 2 is premium • class 3 is control
Step 3	Router(config-tag-cos-map) # exit	Exits the MPLS QoS map submodule.
Step 4	Router(config)# access-list <i>access-list-number</i> permit <i>destination</i>	Creates an access list. The access list acts on traffic going to the specified destination address.
Step 5	Router(config)# tag-switching prefix-map <i>prefix-map</i> access-list <i>access-list</i> cos-map <i>cos-map</i>	Configures the router to use a specified QoS map when an MPLS destination prefix matches the specified access list.

Configuring DWFQ and Changing Queue Weights on an Outgoing Interface

To configure distributed WFQ (dWFQ) and change queue weights on an interface, use the following commands in interface configuration mode after specifying the interface:

	Command	Purpose
Step 1	Router(config)# interface <i>type number</i>	Specifies the interface type and number.
Step 2	Router(config-if)# fair-queue tos	Configures an interface to use fair queuing.
Step 3	Router(config)# fair-queue tos <i>class weight</i>	Changes the class weight on the specified interface.

Verifying QoS Operation

To verify the operation of MPLS QoS, use the following EXEC commands:

	Command	Purpose
Step 1	Router# show tag-switching interfaces <i>interfaces</i>	Displays detailed information about label switching interfaces.
Step 2	Router# show tag-switching cos-map	Displays the QoS map used to assign VCs.
Step 3	Router# show tag-switching prefix-map	Displays the prefix map used to assign a QoS map to network prefixes.

Configuring the MPLS Label Switch Controller

To enable MPLS LSC functionality, perform the tasks described in the following sections. The first two sections are required tasks; the remaining task is optional:

- [Configuring MPLS on the Cisco 7200 Series LSCs for BPX and IGX Switches](#) (Required)
- [Configuring the Cisco 6400 UAC LSC](#) (Required)
- [Verifying MPLS LSC Configuration](#) (Optional)

Refer to the Cisco BPX 8600 or IGX 8400 series documentation for BPX or IGX service node configuration examples.

Configuring MPLS on the Cisco 7200 Series LSCs for BPX and IGX Switches

To configure MPLS on the Cisco 7200 Series LSCs for BPX and IGX switches, use the following commands on each LSC in the configuration beginning in router configuration mode.



Note

If you are configuring for LSC redundancy, ensure that the controller ID matches the slave and is unique to the LSC system. Also, make sure that the VPI/VC value for the control VC matches its peer.

	Command	Purpose
Step 1	Router(config)# interface loopback0 Router(config-if)# ip address 192.103.210.5 255.255.255.255	Enables a loopback interface. A loopback interface provides stable router and LDP identifiers.
Step 2	Router(config)# tag-switching atm disable-headend-vc	Forces the LSC <i>not</i> to assign headend VCs for each destination prefix. With downstream on demand, MPLS ATM networks LVCs are a limited resource that are easily depleted with the addition of each new node.
Step 3	Router(config)# interface atm1/0 Router(config-if)# tag-control-protocol vsi id 1	Enables the VSI protocol on the control interface ATM1/0 with controller ID 1. (Use a unique ID for each LSC.) For the IGX, use the tag-control-protocol vsi slaves 32 id 1 command.

	Command	Purpose
Step 4	Router(config-if)# interface XTagATM61 Router(config-if)# extended-port atm1/0 bpx 6.1	Configures MPLS on the extended label ATM interface by creating an extended label ATM (XTagATM) virtual interface and binding it to BPX port 6.1. For the IGX, use the extended-port atm1/0 descriptor 0.6.1.0 command.
Step 5	Router(config-if)# ip unnumbered loopback0 Router(config-if)# tag-switching atm vpi 2-5 Router(config-if)# tag-switching ip Router(config-if)# exit	Configures MPLS on the extended label ATM interface. Limit the range so that the total number of VPIs does not exceed 4. For example: tag-switching atm vpi 2-5 tag-switching atm vpi 10-13
Step 6	Router(config-if)# interface XTagATM1222 Router(config-if)# extended-port atm1/0 bpx 12.2.2	Configures MPLS on another extended label ATM interface by creating an extended label ATM (XTagATM) virtual interface and binding it to BPX virtual trunk interface 12.2.2. For the IGX, use the extended-port atm1/0 descriptor 0.12.2.2 command.
Step 7	Router(config-if)# ip unnumbered loopback0 Router(config-if)# tag-switching atm vp-tunnel 2 Router(config-if)# tag-switching ip Router(config-if)# exit	Configures MPLS on the extended label ATM interface using a VP-tunnel interface. This will limit the VPI to only vpi = 2. The command will also map tag atm control vc to 2,32.
Step 8	Router(config)# ip cef	Enables CEF switching.

Configuring the Cisco 6400 UAC LSC

To configure a Cisco 6400 UAC LSC, perform the tasks in the following sections. The first section contains a required task; the remaining task is optional:

- [Configuring Cisco 6400 UAC NRP as an MPLS LSC](#) (Required)
- [Configuring the Cisco 6400 UAC NSP for MPLS Connectivity to BPX](#) (Optional)

Configuring Cisco 6400 UAC NRP as an MPLS LSC

To configure a Cisco 6400 UAC NRP as an MPLS LSC, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface loopback0 Router(config-if)# ip address 192.103.210.5 255.255.255.255	Enables a loopback interface. A loopback interface provides stable router and LDP identifiers.
Step 2	Router(config)# interface atm0/0/0 Router(config-if)# tag-control-protocol vsi	Enables the VSI protocol on the control interface ATM0/0/0.

Configuring the MPLS Label Switch Controller

	Command	Purpose
Step 3	Router(config-if)# interface XTagATM61 Router(config-if)# extended-port atm1/0 bpx 6.1	Configures MPLS on the extended label ATM interface by creating an extended label ATM (XTagATM) virtual interface and binding it to BPX port 6.1.
Step 4	Router(config-if)# ip unnumbered loopback0 Router(config-if)# tag-switching atm vpi 2-5 Router(config-if)# tag-switching ip Router(config-if)# exit	Configures MPLS on the extended label ATM interface. Limit the range so that the total number of VPIs does not exceed 4. For example: tag-switching atm vpi 2-5 tag-switching atm vpi 10-13
Step 5	Router(config-if)# interface XTagATM122 Router(config-if)# extended-port atm1/0 bpx 12.2	Configures MPLS on the other extended label ATM interface by creating an extended label ATM (XTagATM) virtual interface and binding it to BPX port 12.2.
Step 6	Router(config-if)# ip unnumbered loopback0 Router(config-if)# tag-switching atm vpi 2-5 Router(config-if)# tag-switching ip Router(config-if)# exit	Configures MPLS on the extended label ATM interface. Limits the range so that the total number of VPIs does not exceed 4. For example: tag-switching atm vpi 2-5 tag-switching atm vpi 10-13
Step 7	Router(config)# ip cef	Enables CEF switching.
Step 8	Router(config)# tag-switching atm disable-headend-vc	Disables headend VC label advertisement.

Configuring the Cisco 6400 UAC NSP for MPLS Connectivity to BPX

To configure a Cisco 6400 UAC NSP for MPLS connectivity to BPX, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Switch# show hardware 3/0 NRP 00-0000-00	Displays the hardware connected to the Cisco 6400 UAC, including the position (3/0) of the NRP in the Cisco 6400 chassis.
Step 2	Switch(config)# interface atm3/0/0	Specifies the ATM interface for which you want to configure PVCs and PVPs.

Command	Purpose
Step 3	<p>Configures the PVC for the VSI control channel, depending on which of the 14 slots in the Cisco BPX is occupied by a Cisco BXM. If you do not know the BPX slots containing a BXM, configure all 14 PVCs to ensure that the NSP functions properly.</p>
<pre>Switch(config-if)# atm pvc 0 40 interface ATM1/0/0 0 40 atm pvc 0 41 interface ATM1/0/0 0 41 atm pvc 0 42 interface ATM1/0/0 0 42 atm pvc 0 43 interface ATM1/0/0 0 43 atm pvc 0 44 interface ATM1/0/0 0 44 atm pvc 0 45 interface ATM1/0/0 0 45 atm pvc 0 46 interface ATM1/0/0 0 46 atm pvc 0 47 interface ATM1/0/0 0 47 atm pvc 0 48 interface ATM1/0/0 0 48 atm pvc 0 49 interface ATM1/0/0 0 49 atm pvc 0 50 interface ATM1/0/0 0 50 atm pvc 0 51 interface ATM1/0/0 0 51 atm pvc 0 52 interface ATM1/0/0 0 52 atm pvc 0 53 interface ATM1/0/0 0 53</pre>	<p> Note Do not enable MPLS on this interface.</p> <p>However, if you know that Cisco BPX slots 10 and 12, for example, contain a BXM, you only need to configure PVCs corresponding to those slots, as follows:</p> <pre>atm pvc 0 49 interface ATM1/0/0 0 49 atm pvc 0 51 interface ATM1/0/0 0 51</pre> <p>Instead of configuring multiple PVCs, you can configure PVP 0 by deleting all well-known VCs. For example, you can use the atm manual-well-known-vc delete command on both interfaces and then configure PVP 0, as follows:</p> <pre>atm pvp 0 interface ATM1/0/0 0</pre>
Step 4	<p>Configures the PVPs for the LVCs. For XTag ATM interfaces, use the VPI range 2 through 5 (by issuing a tag-switching atm vpi 2-5 command). If you want to use some other VPI range, configure the PVPs accordingly.</p>
<pre>Switch(config-if)# atm pvp 2 interface ATM1/0/0 2 atm pvp 3 interface ATM1/0/0 3 atm pvp 4 interface ATM1/0/0 4 atm pvp 5 interface ATM1/0/0 5</pre>	

Verifying MPLS LSC Configuration

To verify your MPLS LSC configuration, use the following commands in EXEC mode:

	Command	Purpose
Step 1	Router# <code>show controller vsi session</code>	Displays the VSI session state.
Step 2	Router# <code>show tag-switching interfaces</code>	Displays the MPLS-enabled interface states.
Step 3	Router# <code>show controllers vsi control-interface</code>	Displays information about an ATM interface that controls an external ATM switch or VSI control interface.
Step 4	Router# <code>show interface XTagATM</code>	Displays information about an extended MPLS ATM interface.
Step 5	Router# <code>show tag-switching tdp discovery</code>	Displays information about the discovery of MPLS neighbors.
Step 6	Router# <code>show tag-switching tdp neighbor</code>	Displays information about the MPLS neighbor relationship.
Step 7	Router# <code>show tag-switching atm capabilities</code>	Displays information about negotiated of TDP or LDP control VPs.
Step 8	Router# <code>show tag-switching atm-tdp bindings</code>	Displays the current headend, tailend, and transit dynamic tag bindings for the destinations.
Step 9	Router# <code>show tag-switching atm-tdp bindwait</code>	Displays the tag VCs that are in bindwait state along with their destinations.
Step 10	Router# <code>show tag-switching atm summary</code>	Displays summary information about the number of destination networks discovered via routing protocol and the LVCs created on each extended label ATM interface.

Configuring MPLS Egress NetFlow Accounting

To configure MPLS egress NetFlow, perform the tasks described in the following sections. The first section contains a required task; the remaining tasks are optional:

- Enabling MPLS Egress NetFlow Accounting (Required)
- Configuring NetFlow Aggregation Cache (Optional)
- [Troubleshooting MPLS Egress NetFlow Accounting](#) (Optional)
- [Verifying MPLS Egress NetFlow Accounting Configuration](#) (Optional)
- [Monitoring and Maintaining MPLS Egress NetFlow Accounting](#) (Optional)

Enabling MPLS Egress NetFlow Accounting

To enable MPLS egress NetFlow accounting, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# mpls netflow egress	Enables MPLS egress NetFlow accounting on the egress router interface.

Configuring NetFlow Aggregation Cache

To configure NetFlow aggregation cache, use the following global configuration command:

Command	Purpose
Router(config)# ip flow-aggregation cache as destination-prefix prefix protocol-port source-prefix	Enters aggregation cache configuration mode and enables an aggregation cache scheme (as, destination-prefix, prefix, protocol-port, or source-prefix). For more information on NetFlow aggregation, see the “Related Documents” section.

Troubleshooting MPLS Egress NetFlow Accounting

To troubleshoot the MPLS egress NetFlow accounting feature, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# show mpls forwarding-table detail	Displays detailed MPLS forwarding-table entries. The output has been modified to show if MPLS egress NetFlow accounting is applied to packets destined to an entry. This is for debugging purposes only.
Router# show mpls interfaces internal all	Displays detailed information about all of the MPLS interfaces in the router. The output has been modified to show if MPLS egress NetFlow accounting is enabled on the interface. This is for debugging purposes only.

Verifying MPLS Egress NetFlow Accounting Configuration

To verify MPLS egress NetFlow accounting configuration, perform the following steps:

- Step 1** Enter the **show ip cache flow** EXEC command to display a summary of NetFlow switching statistics.



Note This is an existing command that displays ingress and egress NetFlow statistics.

```
Router# show ip cache flow
```

```
IP packet size distribution (10 total packets):
```

```

1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
.000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
 1 active, 65535 inactive, 2 added
 26 ager polls, 0 flow alloc failures
 last clearing of statistics never
Protocol      Total    Flows    Packets Bytes    Packets Active(Sec) Idle(Sec)
-----      -
              Flows    /Sec     /Flow  /Pkt    /Sec    /Flow    /Flow
ICMP          1        0.0      5     100     0.0     0.0     15.7
Total :      1        0.0      5     100     0.0     0.0     15.7

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Et1/1      34.0.0.2      Et1/4      180.1.1.2     01 0000 0800 5

```

Table 5 describes the fields in the flow switching cache lines of the output.

Table 5 *show ip cache flow Field Descriptions—Flow Switching Cache*

Field	Description
IP packet size distribution	The two lines below this banner show the percentage distribution of packets by size range.
bytes	Number of bytes of memory the NetFlow cache uses.
active	Number of active flows in the NetFlow cache at the time this command is entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache but are not assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to remove expired entries (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
last clearing of statistics	Standard time output (hh:mm:ss) since the clear ip flow stats EXEC command was executed. This time output changes to hours and days after 24 hours is exceeded.

Table 6 describes the fields in the activity-by-protocol lines of the output.

Table 6 *show ip cache flow Field Descriptions—Activity-by-Protocol*

Field	Description
Protocol	IP protocol and the “well known” port number as described in RFC 1340.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol seen per second; equal to total flows/number of seconds for this summary period.

Table 6 *show ip cache flow Field Descriptions—Activity-by-Protocol (continued)*

Field	Description
Packets/Flow	Average number of packets observed for the flows seen for this protocol. Equal to total packets for this protocol/number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol and the total number of packet for this protocol for this summary period).
Packets/Sec	Average number of packets for this protocol per second (total packets for this protocol and the total number of seconds for this summary period).
Active(Sec)/Flow	Sum of all the seconds from the first packet to the last packet of an expired flow (for example, TCP FIN, time out, and so on) in seconds/total flows for this protocol for this summary period.
Idle(Sec)/Flow	Sum of all the seconds from the last packet seen in each nonexpired flow for this protocol until the time this command was entered, in seconds/total flows for this protocol for this summary period.

Table 7 describes the fields in the current flow lines of the output.

Table 7 *show ip cache flow Field Descriptions—Current Flow*

Field	Description
SrcIf	Internal port name of the router for the source interface.
SrcIPAddress	Source IP address for this flow.
DstIf	Internal port name of the router for the destination interface.
DstIPAddress	Destination IP address for this flow.
Pr	IP protocol; for example, 6 = TCP, 17 = UDP, ... as defined in RFC 1340.
SrcP	Source port address, TCP/UDP “well known” port number, as defined in RFC 1340.
DstP	Destination port address, TCP/UDP “well known” port number, as defined in RFC 1340.
Pkts	Number of packets that the router observed for this flow.

Step 2 Enter the **show ip cache flow aggregation** EXEC command to display the contents of the aggregation cache. To display the prefix-based aggregation cache, use the following EXEC commands:

```
Router# show ip cache flow agg
Router# show ip cache flow aggregation pref
Router# show ip cache flow aggregation prefix
```

```
IP Flow Switching Cache, 278544 bytes
 1 active, 4095 inactive, 1 added
 4 ager polls, 0 flow alloc failures
```

```
Src If      Src Prefix  Msk  Dst If      Dst Prefix  Msk  Flows  Pkts
Et1/1      34.0.0.0   /8   Et1/4      180.1.1.0   /24   1     5
```

Router#

Table 8 describes the fields in the flow switching cache lines of the output.

Table 8 *show ip cache flow aggregation prefix Field Descriptions—Flow Switching Cache*

Field	Description
bytes	Number of bytes of memory the NetFlow cache uses.
active	Number of active flows in the NetFlow cache at the time this command is entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache but are not assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to remove expired entries (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.

Table 9 describes the fields in the current flow lines of the output.

Table 9 *show ip cache flow aggregation prefix Field Descriptions—Current Flow*

Field	Description
Src If	Router's internal port name for the source interface.
Src Prefix	Source IP address for this flow.
Msk	Mask source.
Dst If	Router's internal port name for the destination interface.
Dst Prefix	Destination prefix aggregation cache scheme.
Msk	Mask destination.
Flows	Number of flows.
Pkts	Number of packets that the router observed for this flow.

The **ip flow-aggregation cache** command has other options, including the following:

{as | destination-prefix | prefix | protocol-port | source-prefix }



Note

For more information on these options, refer to the *NetFlow Aggregation* documentation.

Here is sample configuration output from the NetFlow aggregation cache:

```
Router(config)# ip flow-agg
Router(config)# ip flow-aggregation cache
Router(config)# ip flow-aggregation cache ?
  as                AS aggregation
  destination-prefix Destination Prefix aggregation
  prefix            Prefix aggregation
```

```
protocol-port      Protocol and port aggregation
source-prefix     Source Prefix aggregation
```

```
Router(config)# ip flow-aggregation cache prefix
Router(config-flow-cache)# enable
```

Here is sample output displaying the IP aggregation cache contents:

```
Router# show ip cache flow aggregation ?
as                AS aggregation cache
destination-prefix Destination Prefix aggregation cache
prefix           Source/Destination Prefix aggregation cache
protocol-port    Protocol and port aggregation cache
source-prefix    Source Prefix aggregation cache
Router# show ip cache flow
IP packet size distribution (206 total packets):
  1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
    .000 .854 .000 .145 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4292920 bytes
  0 active, 62977 inactive, 182 added
  2912 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol      Total      Flows      Packets Bytes      Packets Active(Sec) Idle(Sec)
-----      -
              Flows      /Sec       /Flow  /Pkt       /Sec      /Flow /Flow
ICMP          182        0.0        1      62         0.0       0.0 15.5
Total :      182        0.0        1      62         0.0       0.0 15.5

SrcIf          SrcIPAddress  DstIf          DstIPAddress   Pr SrcP DstP  Pkts

Router# show ip cache flow aggregation prefix

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 3 added
  45 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds

Src If          Src Prefix    Msk Dst If          Dst Prefix    Msk Flows  Pkts
Et1/1          34.0.0.0     /8  P06/0             12.12.12.12   /32 1        5
Router#
```

Monitoring and Maintaining MPLS Egress NetFlow Accounting

To monitor and maintain MPLS egress NetFlow accounting, use the following command in EXEC mode:

Command	Purpose
Router# show ip cache flow	Displays summary NetFlow switching statistics, including the size of the packets, types of traffic, which interfaces the traffic enters and exits, and the source and destination addresses in the forwarded packet.

Verifying Configuration of MPLS Forwarding

To verify that CEF has been configured properly, enter the **show ip cef summary** command, which generates output similar to the following:

```
Router# show ip cef summary

IP CEF with switching (Table Version 49), flags=0x0
 43 routes, 0 resolve, 0 unresolved (0 old, 0 new)
 43 leaves, 49 nodes, 56756 bytes, 45 inserts, 2 invalidations
 2 load sharing elements, 672 bytes, 2 references
 1 CEF resets, 4 revisions of existing leaves
 4 in-place modifications
 refcounts: 7241 leaf, 7218 node

Adjacency Table has 18 adjacencies
Router#
```

MPLS Configuration Examples

This section provides the following MPLS configuration examples:

- [Enabling MPLS Incrementally in a Network Example](#)
- [Enabling MPLS for a Subset of Destination Prefixes Example](#)
- [Selecting the Destination Prefixes and Paths Example](#)
- [Displaying MPLS LDP Binding Information Example](#)
- [Displaying MPLS Forwarding Table Information Example](#)
- [Displaying MPLS Interface Information Example](#)
- [Displaying MPLS LDP Neighbor Information Example](#)
- [Enabling LSP Tunnel Signalling Example](#)
- [Configuring an LSP Tunnel Example](#)
- [Displaying the LSP Tunnel Information Example](#)
- [Configuring MPLS Traffic Engineering Examples](#)
- [Configuring MPLS VPNs Example](#)
- [Implementing MPLS QoS Example](#)
- [Configuring an MPLS LSC Examples](#)
- [MPLS Egress NetFlow Accounting Example](#)

Enabling MPLS Incrementally in a Network Example

The following example shows how to configure MPLS incrementally throughout a network of routers. You enable MPLS first between one pair of routers (in this case, R1 and R3 shown in [Figure 1](#)) and add routers step by step until every router in the network is label switch enabled.

```
router-1# configuration terminal
router-1(config)# ip cef distributed
router-1(config)# tag-switching ip
router-1(config)# interface e0/1
```

```
router-1(config-if)# tag-switching ip
router-1(config-if)# exit
router-1(config)#
router-3# configuration terminal
router-3(config)# ip cef distributed
router-3(config)# tag-switching ip
router-3(config)# interface e0/1
router-3(config-if)# tag-switching ip
router-3(config-if)# exit
router-3(config)#
```

Enabling MPLS for a Subset of Destination Prefixes Example

The following example shows the commands you enter at each of the routers to enable MPLS for only a subset of destination prefixes (see [Figure 1](#)).

```
Router(config)# access-list-1 permit A
Router(config)# tag-switching advertise-tags for 1
```

Selecting the Destination Prefixes and Paths Example

The following example shows the commands you enter to configure the routers to select the destination prefixes and paths for which MPLS is enabled. When you configure R2, R5, and R8 to distribute no labels to other routers, you ensure that no routers send them labeled packets. You also need to configure routers R1, R3, R4, R6, and R7 to distribute labels only for network A and only to the applicable adjacent router. This configuration ensures that R3 distributes its label for network A only to R1, R4 only to R3, R6 only to R4, and R7 only to R6 (see [Figure 1](#)).

```
router-2(config)# no tag-switching advertise-tags
router-5(config)# no tag-switching advertise-tags
router-8(config)# no tag-switching advertise-tags
router-1(config)# access-list permit R1
router-1(config)# no tag-switching advertise-tags for 1
router-1(config)# tag-switching advertise-tags for 1 to 2
router-1(config)# exit

router-3# access-list 1 permit A
router-3# access-list 2 permit R1
router-3# tag-switching advertise-tags for 1 to 2
router-3# exit

router-4# access-list 1 permit A
router-4# access-list 2 permit R3
router-4# tag-switching advertise-tags for 1 to 2
router-4# exit

router-6# access-list 1 permit A
router-6# access-list 2 permit R4
router-6# tag-switching advertise-tags for 1 to 2
router-6# exit
router-7# access-list 1 permit A
router-7# access-list 2 permit R6
router-7# tag-switching advertise-tags for 1 to 2
router-7# exit
```

Displaying MPLS LDP Binding Information Example

The following example shows how to use the **show tag-switching tdp bindings EXEC** command to display the contents of the Label Information Base (LIB). The display can show the entire database or can be limited to a subset of entries, based on prefix, input or output label values or ranges, or the neighbor advertising the label.



Note

This command displays downstream mode bindings. For label VC bindings, see the **show tag-switching atm-tdp bindings EXEC** command.

```
Router# show tag-switching tdp bindings

Matching entries:
tib entry: 10.92.0.0/16, rev 28
    local binding: tag: imp-null(1)
    remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 10.102.0.0/16, rev 29
    local binding: tag: 26
    remote binding: tsr: 172.27.32.29:0, tag: 26
tib entry: 10.105.0.0/16, rev 30
    local binding: tag: imp-null(1)
    remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 10.205.0.0/16, rev 31
    local binding: tag: imp-null(1)
    remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 10.211.0.7/32, rev 32
    local binding: tag: 27
    remote binding: tsr: 172.27.32.29:0, tag: 28
tib entry: 10.220.0.7/32, rev 33
    local binding: tag: 28
    remote binding: tsr: 172.27.32.29:0, tag: 29
tib entry: 99.101.0.0/16, rev 35
    local binding: tag: imp-null(1)
    remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 100.101.0.0/16, rev 36
    local binding: tag: 29
    remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 171.69.204.0/24, rev 37
    local binding: tag: imp-null(1)
    remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 172.27.32.0/22, rev 38
    local binding: tag: imp-null(1)
    remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 210.10.0.0/16, rev 39
    local binding: tag: imp-null(1)
tib entry: 210.10.0.8/32, rev 40
    remote binding: tsr: 172.27.32.29:0, tag: 27
```

Displaying MPLS Forwarding Table Information Example

The following example shows how to use the **show tag-switching forwarding-table** command to display the contents of the LFIB. The LFIB lists the labels, output interface information, prefix or tunnel associated with the entry, and number of bytes received with each incoming label. A request can show the entire LFIB or can be limited to a subset of entries. A request can also be restricted to selected entries in any of the following ways:

- Single entry associated with a given incoming label

- Entries associated with a given output interface
- Entries associated with a given next hop
- Single entry associated with a given destination
- Single entry associated with a given tunnel having the current node as an intermediate hop

```
Router# show tag-switching forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
26	Untagged	10.253.0.0/16	0	Et4/0/0	172.27.32.4
28	1/33	10.15.0.0/16	0	AT0/0.1	point2point
29	Pop tag	10.91.0.0/16	0	Hs5/0	point2point
	1/36	10.91.0.0/16	0	AT0/0.1	point2point
30	32	10.250.0.97/32	0	Et4/0/2	10.92.0.7
	32	10.250.0.97/32	0	Hs5/0	point2point
34	26	10.77.0.0/24	0	Et4/0/2	10.92.0.7
	26	10.77.0.0/24	0	Hs5/0	point2point
35	Untagged [T]	10.100.100.101/32	0	Tu301	point2point
36	Pop tag	168.1.0.0/16	0	Hs5/0	point2point
	1/37	168.1.0.0/16	0	AT0/0.1	point2point

```
[T] Forwarding through a TSP tunnel.  
View additional tagging info with the 'detail' option
```

Displaying MPLS Interface Information Example

The following example shows how to use the **show tag-switching interfaces** command to show information about the requested interface or about all interfaces on which MPLS is enabled. The per-interface information includes the interface name and indications as to whether IP MPLS is enabled and operational.

```
Router# show tag-switching interfaces
```

Interface	IP	Tunnel	Operational
Hssi3/0	Yes	Yes	No
ATM4/0.1	Yes	Yes	Yes (ATM tagging)
Ethernet5/0/0	No	Yes	Yes
Ethernet5/0/1	Yes	No	Yes
Ethernet5/0/2	Yes	No	No
Ethernet5/0/3	Yes	No	Yes
Ethernet5/1/1	Yes	No	No

The following shows sample output from the **show tag-switching interfaces** command when you specify the **detail** keyword:

```
Router# show tag-switching interfaces detail
```

```
Interface Hssi3/0:
  IP tagging enabled
  TSP Tunnel tagging enabled
  Tagging not operational
  MTU = 4470
Interface ATM4/0.1:
  IP tagging enabled
  TSP Tunnel tagging enabled
  Tagging operational
  MTU = 4470
  ATM tagging: Tag VPI = 1, Control VC = 0/32
Interface Ethernet5/0/0:
  IP tagging not enabled
```

```

TSP Tunnel tagging enabled
Tagging operational
MTU = 1500
Interface Ethernet5/0/1:
  IP tagging enabled
  TSP Tunnel tagging not enabled
  Tagging operational
  MTU = 1500
Interface Ethernet5/0/2:
  IP tagging enabled
  TSP Tunnel tagging not enabled
  Tagging not operational
  MTU = 1500
Interface Ethernet5/0/3:
  IP tagging enabled
  TSP Tunnel tagging not enabled
  Tagging operational
  MTU = 1500

```

Displaying MPLS LDP Neighbor Information Example

The following example shows how to use the **show tag-switching tdp neighbors EXEC** command to display the status of LDP sessions. The neighbor information branch can have information about all LDP neighbors or can be limited to the neighbor with a specific IP address or LDP identifier, or to LDP neighbors known to be accessible over a specific interface.

```

Router# show tag-switching tdp neighbors

Peer TDP Ident: 10.220.0.7:1; Local TDP Ident 172.27.32.29:1
  TCP connection: 10.220.0.7.711 - 172.27.32.29.11029
  State: Oper; PIEs sent/rcvd: 17477/17487; Downstream on demand
Up time: 01:03:00
TDP discovery sources:
  ATM0/0.1
Peer TDP Ident: 210.10.0.8:0; Local TDP Ident 172.27.32.29:0
  TCP connection: 210.10.0.8.11004 - 172.27.32.29.711
  State: Oper; PIEs sent/rcvd: 14656/14675; Downstream;
Up time: 2d5h
TDP discovery sources:
  Ethernet4/0/1
  Ethernet4/0/2
  POS6/0/0
Addresses bound to peer TDP Ident:
  99.101.0.8      172.27.32.28    10.105.0.8      10.92.0.8
  10.205.0.8     210.10.0.8

```

Enabling LSP Tunnel Signalling Example

The following example shows how to configure support for LSP tunnel signalling along a path and on each interface crossed by one or more tunnels:

```

Router(config)# ip cef distributed
Router(config)# tag-switching tsp-tunnels
Router(config)# interface e0/1
Router(config-if)# tag-switching tsp-tunnels
Router(config-if)# interface e0/2
Router(config-if)# tag-switching tsp-tunnels
Router(config-if)# exit

```

Configuring an LSP Tunnel Example

The following example shows how to set the encapsulation of the tunnel to MPLS and how to define hops in the path for the LSP.

Follow these steps to configure a two-hop tunnel, hop 0 being the headend router. For hops 1 and 2, you specify the IP addresses of the incoming interfaces for the tunnel. The tunnel interface number is arbitrary, but must be less than 65,535.

```
Router(config)# interface tunnel 2003
Router(config-if)# tunnel mode tag-switching
Router(config-if)# tunnel tsp-hop 1 10.10.0.12
Router(config-if)# tunnel tsp-hop 2 10.50.0.24 lasthop
Router(config-if)# exit
```

To shorten the previous path, delete the hop by entering the following commands:

```
Router(config)# interface tunnel 2003
Router(config-if)# no tunnel tsp-hop 2
Router(config-if)# tunnel tsp-hop 1 10.10.0.12 lasthop
Router(config-if)# exit
```

Displaying the LSP Tunnel Information Example

The following example shows how to use the **show tag-switching tsp-tunnels** command to display information about the configuration and status of selected tunnels:

```
Router# show tag-switching tsp-tunnels

Signalling Summary:
    TSP Tunnels Process:      running
    RSVP Process:            running
    Forwarding:               enabled

TUNNEL ID DESTINATION      STATUS      CONNECTION
10.106.0.6.200310.2.0.12up  up
```

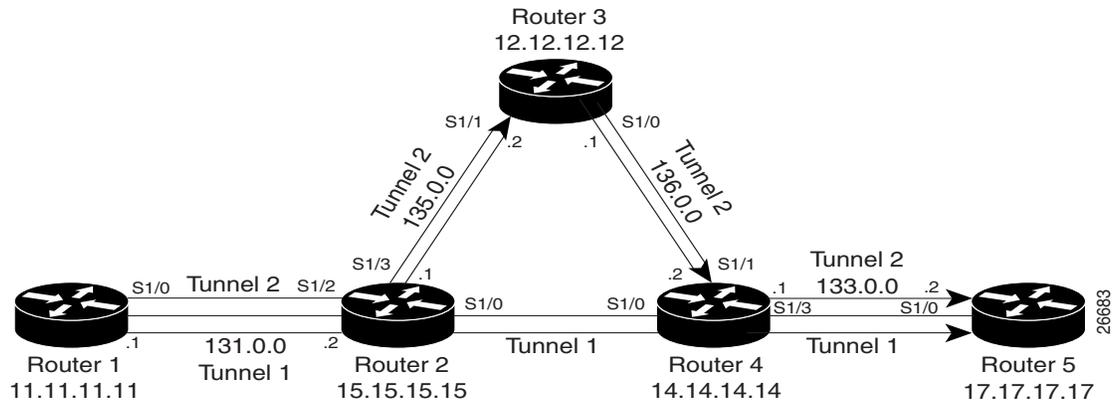
Configuring MPLS Traffic Engineering Examples

This section provides the following MPLS traffic engineering configuration examples:

- [Configuring MPLS Traffic Engineering Using IS-IS Example](#)
- [Configuring MPLS Traffic Engineering Using OSPF Example](#)
- [Configuring an MPLS Traffic Engineering Tunnel Example](#)
- [Configuring Enhanced SPF Routing over a Tunnel Example](#)

Figure 3 illustrates a sample MPLS topology. This example specifies point-to-point outgoing interfaces. The next sections contain sample configuration commands you enter to implement MPLS traffic engineering and the basic tunnel configuration shown in **Figure 3**.

Figure 3 Sample MPLS Traffic Engineering Tunnel Configuration



Configuring MPLS Traffic Engineering Using IS-IS Example

This example lists the commands you enter to configure MPLS traffic engineering with IS-IS routing enabled (see [Figure 3](#)).



Note

You must enter the following commands on every router in the traffic-engineered portion of your network.

Router 1—MPLS Traffic Engineering Configuration

To configure MPLS traffic engineering, enter the following commands:

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 11.11.11.11 255.255.255.255
ip router isis

interface s1/0
ip address 131.0.0.1 255.255.0.0
ip router isis
mpls traffic-eng tunnels
ip rsvp bandwidth 1000
```

Router 1—IS-IS Configuration

To enable IS-IS routing, enter the following commands:

```
router isis
network 47.0000.0011.0011.00
is-type level-1
metric-style wide
mpls traffic-eng router-id loopback0
mpls traffic-eng level-1
```

Configuring MPLS Traffic Engineering Using OSPF Example

This example lists the commands you enter to configure MPLS traffic engineering with OSPF routing enabled (see [Figure 3](#)).

**Note**

You must enter the following commands on every router in the traffic-engineered portion of your network.

Router 1—MPLS Traffic Engineering Configuration

To configure MPLS traffic engineering, enter the following commands:

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 11.11.11.11 255.255.255.255

interface s1/0
ip address 131.0.0.1 255.255.0.0
mpls traffic-eng tunnels
  ip rsvp bandwidth 1000
```

Router 1—OSPF Configuration

To enable OSPF, enter the following commands:

```
router ospf 0
network 131.0.0.0.0.0.255.255 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
```

Configuring an MPLS Traffic Engineering Tunnel Example

This example shows you how to configure a dynamic path tunnel and an explicit path in the tunnel. Before you configure MPLS traffic engineering tunnels, you must enter the appropriate global and interface commands on the specified router (in this case, Router 1).

Router 1—Dynamic Path Tunnel Configuration

In this section, a tunnel is configured to use a dynamic path:

```
interface tunnell
  ip unnumbered loopback 0
  tunnel destination 17.17.17.17
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng bandwidth 100
  tunnel mpls traffic-eng priority 1 1
  tunnel mpls traffic-eng path-option 1 dynamic
```

Router 1—Dynamic Path Tunnel Verification

This section includes the commands you use to verify that the tunnel is up:

```
show mpls traffic-eng tunnels
show ip interface tunnell
```

Router 1—Explicit Path Configuration

In this section, an explicit path is configured:

```
ip explicit-path identifier 1
  next-address 131.0.0.1
  next-address 135.0.0.1
  next-address 136.0.0.1
  next-address 133.0.0.1
```

Router 1—Explicit Path Tunnel Configuration

In this section, a tunnel is configured to use an explicit path:

```
interface tunnel2
  ip unnumbered loopback 0
  tunnel destination 17.17.17.17
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng bandwidth 100
  tunnel mpls traffic-eng priority 1 1
  tunnel mpls traffic-eng path-option 1 explicit identifier 1
```

Router 1—Explicit Path Tunnel Verification

This section includes the commands you use to verify that the tunnel is up:

```
show mpls traffic-eng tunnels
show ip interface tunnel2
```

Configuring Enhanced SPF Routing over a Tunnel Example

This section includes the commands that cause the tunnel to be considered by the enhanced SPF calculation of the IGP, which installs routes over the tunnel for appropriate network prefixes.

Router 1—IGP Enhanced SPF Consideration Configuration

In this section, you specify that the IGP should use the tunnel (if the tunnel is up) in its enhanced SPF calculation:

```
interface tunnell
  tunnel mpls traffic-eng autoroute announce
```

Router 1—Route and Traffic Verification

This section includes the commands you use to verify that the tunnel is up and that the traffic is routed through the tunnel:

```
show traffic-eng tunnels tunnell brief
show ip route 17.17.17.17
show mpls traffic-eng autoroute
ping 17.17.17.17
show interface tunnell accounting
show interface s1/0 accounting
```

Configuring MPLS VPNs Examples

This section provides the following configuration examples:

- [Configuring MPLS VPNs Example](#)
- [Defining a Cable Subinterface Example](#)
- [Cable Interface Bundling Example](#)
- [Subinterface Definition on Bundle Master Example](#)
- [Cable Interface Bundle Master Configuration Example](#)
- [Configuring EBGp Routing to Exchange VPN Routes Between Autonomous Systems](#)
- [Configuring EBGp Routing to Exchange VPN Routes Between Autonomous Systems in a Confederation](#)

Configuring MPLS VPNs Example

The following example provides a sample configuration file from a PE router:

```
ip cef distributed          ! CEF switching is pre-requisite for label Switching
frame-relay switching
!
ip vrf vrf1                ! Define VPN Routing instance vrf1
 rd 100:1
  route-target both 100:1  ! Configure import and export route-targets for vrf1
!
ip vrf vrf2                ! Define VPN Routing instance vrf2
 rd 100:2
  route-target both 100:2  ! Configure import and export route-targets for vrf2
  route-target import 100:1 ! Configure an additional import route-target for vrf2
  import map vrf2_import   ! Configure import route-map for vrf2
!
interface lo0
 ip address 10.13.0.13 255.255.255.255
!
interface atm9/0/0        ! Backbone link to another Provider router
!
interface atm9/0/0.1 tag-switching
 ip unnumbered loopback0
  no ip directed-broadcast
  tag-switching atm vpi 2-5
  tag-switching ip
!
interface atm5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface Ethernet1/0
 ip address 3.3.3.5 255.255.0.0
 no ip directed-broadcast
 no ip mroute-cache
 no keepalive
!
interface Ethernet5/0/1  ! Set up Ethernet interface as VRF link to a CE router
 ip vrf forwarding vrf1
 ip address 10.20.0.13 255.255.255.0
!
interface hssi 10/1/0

 hssi internal-clock
 encaps fr
 frame-relay intf-type dce
```

```

frame-relay lmi-type ansi
!
interface hssi 10/1/0.16 point-to-point
 ip vrf forwarding vrf2
 ip address 10.20.1.13 255.255.255.0
 frame-relay interface-dlci 16 ! Set up Frame Relay PVC subinterface as link to another
!                               ! CE router

router bgp 1                      ! Configure BGP sessions
 no synchronization
 no bgp default ipv4-activate      ! Deactivate default IPv4 advertisements
 neighbor 10.15.0.15 remote-as 1   ! Define IBGP session with another PE
 neighbor 10.15.0.15 update-source lo0
!
 address-family vpnv4 unicast      ! Activate PE exchange of VPNv4 NLRI
  neighbor 10.15.0.15 activate
  exit-address-family
!
 address-family ipv4 unicast vrf vrf1 ! Define BGP PE-CE session for vrf1
  redistribute static
   redistribute connected
  neighbor 10.20.0.60 remote-as 65535
  neighbor 10.20.0.60 activate
  no auto-summary
  exit-address-family
!
 address-family ipv4 unicast vrf vrf2 ! Define BGP PE-CE session for vrf2
  redistribute static
   redistribute connected
  neighbor 10.20.1.11 remote-as 65535
  neighbor 10.20.1.11 update-source h10/1/0.16
  neighbor 10.20.1.11 activate
  no auto-summary
  exit-address-family
!
! Define a VRF static route
 ip route vrf vrf1 12.0.0.0 255.0.0.0 e5/0/1 10.20.0.60
!
 route-map vrf2_import permit 10    ! Define import route-map for vrf2.
 ...

```

Defining a Cable Subinterface Example

The following example shows how to define a subinterface on cable3/0:

```

interface cable3/0
! No IP address
! MAC level configuration only

! first subinterface
interface cable3/0.1
 description Management Subinterface
 ip address 10.255.1.1 255.255.255.0
 cable helper-address 10.151.129.2

! second subinterface
interface cable3/0.2
 ip address 10.279.4.2 255.255.255.0
 cable helper-address 10.151.129.2

! third subinterface
interface cable3/0.3
 ip address 10.254.5.2 255.255.255.0

```

```
cable helper-address 10.151.129.2
```

Cable Interface Bundling Example

The following example shows how to bundle a group of physical interfaces:

```
interface c3/0 and interface c4/0 are bundled.

interface c3/0
ip address 209.165.200.225 255.255.255.0
ip address 209.165.201.1 255.255.255.0 secondary
cable helper-address 10.5.1.5
! MAC level configuration
cable bundle 1 master
int c4/0
! No IP address
! MAC layer configuration only
cable bundle 1
```

Subinterface Definition on Bundle Master Example

The following example shows how to define subinterfaces on a bundle master and define Layer 3 configurations for each subinterface:

interface c3/0 and interface c4/0 are bundled.

```
interface c3/0
! No IP address
! MAC level configuration only
cable bundle 1 master

interface c4/0
! No IP address
! MAC layer configuration
cable bundle 1

! first subinterface
interface c3/0.1
ip address 10.22.64.0 255.255.255.0
cable helper-address 10.4.1.2

! second subinterface
interface c3/0.2
ip address 10.12.39.0 255.255.255.0
cable helper-address 10.4.1.2

! third subinterface
interface c3/0.3
ip address 10.96.3.0 255.255.255.0
cable helper-address 10.4.1.2
```

Cable Interface Bundle Master Configuration Example

The following examples show how to configure cable interface bundles:

```
Displaying the contents of the bundle
Router(config-if)# cable bundle ?
  <1-255> Bundle number
Router(config-if)# cable bundle 25 ?
  master Bundle master
  <cr>
```

```

Router(config-if)# cable bundle 25 master ?
<cr>
Router(config-if)# cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up

```

PE Router Configuration Example

```

!
! Identifies the version of Cisco IOS software installed.
version 12.0

! Defines the hostname of the Cisco uBR7246
hostname region-1-ubr
!
! Describes where the system is getting the software image it is running. In
! this configuration example, the system is loading a Cisco uBR7246 image named
! AdamSpecial from slot 0.
boot system flash slot0:ubr7200-p-mz.AdamSpecial
!
! Creates the enable secret password.
enable secret xxxx
enable password xxxx
!
! Sets QoS per modem for the cable plant.
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
! Allows the system to use a full range of IP addresses, including subnet zero, for
! interface addresses and routing updates.
ip subnet-zero
!
! Enables Cisco Express Forwarding.
ip cef
!
! Configures a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to insert the
! DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information option
!
! Enters the virtual routing forwarding (VRF) configuration mode and maps a VRF table to
! the virtual private network (VPN) called MGMT-VPN. The VRF table contains the set of
! routes that points to or gives routes to the CNR device, which provisions the cable
! modem devices. Each VRF table defines a path through the MPLS cloud.
ip vrf MGMT-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
rd 100:1
!
! Creates a list of import and/or export route target communities for the VPN.
route-target export 100:2
route-target export 100:3
!
! Maps a VRF table to the VPN called ISP1-VPN.
ip vrf ISP1-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
rd 100:2
!
! Creates a list of import and/or export route target communities for the VPN.
route-target import 100:1

```

```
!
! Maps a VRF table to the VPN called ISP2-VPN.
ip vrf ISP2-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
  rd 100:3
!
! Creates a list of import and/or export route target communities for the VPN.
  route-target import 100:1
!
! Maps a VRF table to the VPN called MSO-isp. Note: MSO-isp could be considered ISP-3; in
! this case, the MSO is competing with other ISPs for other ISP services.
ip vrf MSO-isp
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
  rd 100:4
!
! Creates a list of import and/or export route target communities for the VPN.
  route-target import 100:1
!
! Builds a loopback interface to be used with MPLS and BGP; creating a loopback interface
! eliminates unnecessary updates (caused by physical interfaces going up and down) from
! flooding the network.
interface Loopback0
  ip address 10.0.0.0 255.255.255.0
  no ip directed-broadcast
!
! Assigns an IP address to this Fast Ethernet interface. MPLS tag-switching must be
! enabled on this interface.
interface FastEthernet0/0
  description Connection to MSO core.
  ip address 10.0.0.0 255.255.255.0
  no ip directed-broadcast
  full-duplex
  tag-switching ip
!
! Enters cable interface configuration mode and configures the physical aspects of the
! 3/0 cable interface. Please note that no IP addresses are assigned to this interface;
! they will be assigned instead to the logical subinterfaces. All other commands for
! this cable interface should be configured to meet the specific needs of your cable RF
! plant and cable network.
interface Cable3/0
  no ip address
  ip directed-broadcast
  no ip mroute-cache
  load-interval 30
  no keepalive
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 855000000
  cable upstream 0 frequency 300000000
  cable upstream 0 power-level 0
  no cable upstream 0 shutdown
  cable upstream 1 shutdown
  cable upstream 2 shutdown
  cable upstream 3 shutdown
  cable upstream 4 shutdown
  cable upstream 5 shutdown
!
! Configures the physical aspects of the 3/0.1 cable subinterface. If cable modems have
! not been assigned IP addresses, they will automatically come on-line using the settings
```

```

! for subinterface X.1.
interface Cable3/0.1
  description Cable Administration Network
!
! Associates this interface with the VRF and MPLS VPNs that connect to the MSO cable
! network registrar (CNR). The CNR provides cable modems with IP addresses and other
! initialization parameters.
  ip vrf forwarding MSO
!
! Defines a range of IP addresses and masks to be assigned to cable modems not yet
! associated with an ISP.
  ip address 10.0.0.0 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
  no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
  cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PCs that are not yet associated with an ISP.
  cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
  no cable proxy-arp
  no cable ip-multicast-echo
!
! Configures the physical aspects of the 3/0.2 cable subinterface.
interface Cable3/0.2
  description MSO as ISP Network
!
! Assigns this subinterface to the MPLS VPN used by the MSO to supply service to
! customers—in this case, MSO-isp.
  ip vrf forwarding MSO-isp
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
  ip address 10.1.0.0 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
  ip address 10.1.0.0 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
  no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
  cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
  cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
  no cable proxy-arp
  no cable ip-multicast-echo
!
! Configures the physical aspects of the 3/0.3 cable subinterface
interface Cable3/0.3
  description ISP1's Network
!
! Makes this subinterface a member of the MPLS VPN.

```

```

ip vrf forwarding isp1
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
ip address 10.1.1.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
no ip directed-broadcast
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
no cable proxy-arp
no cable ip-multicast-echo
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
cable helper-address 10.4.1.2 host
!
! Configures the physical aspects of the 3/0.4 cable subinterface
interface Cable3/0.4
description ISP2's Network
!
! Makes this subinterface a member of the MPLS VPN.
ip vrf forwarding isp2
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
ip address 10.1.2.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
no ip directed-broadcast
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
no cable proxy-arp
no cable ip-multicast-echo
!
!
cable dhcp-giaddr policy
!
!! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
cable helper-address 10.4.1.2 host
!
!
end

```

P Router Configuration Example

Building configuration...

```

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R7460-7206-02
!
enable password xxxx
!
ip subnet-zero
ip cef
ip host brios 223.255.254.253
!
interface Loopback0
 ip address 10.2.1.3 255.255.255.0
 no ip directed-broadcast
!
interface Loopback1
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 1.7.108.2 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 full-duplex
 no cdp enable
!
interface Ethernet1/0
 ip address 10.0.1.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 tag-switching ip
 no cdp enable
!
interface Ethernet1/1
 ip address 10.0.1.17 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 tag-switching ip
 no cdp enable
!
interface Ethernet1/2
 ip address 10.0.2.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 tag-switching ip
 no cdp enable
!
interface Ethernet1/3
 ip address 10.0.3.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 tag-switching ip
 no cdp enable

```

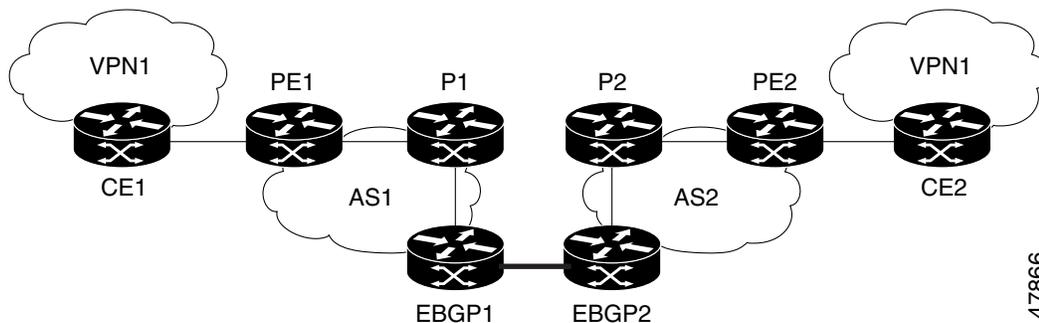
```
!  
interface Ethernet1/4  
 ip address 10.0.4.2 255.255.255.0  
 no ip directed-broadcast  
 no ip route-cache cef  
 no ip mroute-cache  
 tag-switching ip  
 no cdp enable  
!  
interface Ethernet1/5  
 no ip address  
 no ip directed-broadcast  
 no ip route-cache cef  
 shutdown  
 no cdp enable  
!  
interface Ethernet1/6  
 no ip address  
 no ip directed-broadcast  
 no ip route-cache cef  
 shutdown  
 no cdp enable  
!  
interface Ethernet1/7  
 no ip address  
 no ip directed-broadcast  
 no ip route-cache cef  
 shutdown  
 no cdp enable  
!  
router ospf 222  
 network 10.0.1.0 255.255.255.0 area 0  
 network 10.0.2.0 255.255.255.0 area 0  
 network 10.0.3.0 255.255.255.0 area 0  
 network 10.0.4.0 255.255.255.0 area 0  
 network 20.2.1.3 255.255.255.0 area 0  
!  
ip classless  
no ip http server  
!  
!  
map-list test-b  
no cdp run  
!  
tftp-server slot0:master/120/c7200-p-mz.120-1.4  
!  
line con 0  
 exec-timeout 0 0  
 password xxxx  
 login  
 transport input none  
line aux 0  
line vty 0 4  
 password xxxx  
 login  
!  
no scheduler max-task-time  
end
```

Configuring EBGp Routing to Exchange VPN Routes Between Autonomous Systems

The network topology in [Figure 4](#) shows two autonomous systems, which are configured as follows:

- Autonomous system 1 (AS1) includes PE1, P1, EBG1. The IGP is OSPF.
- Autonomous system 2 (AS2) includes PE2, P2, EBG2. The IGP is ISIS.
- CE1 and CE2 belongs to the same VPN, which is called VPN1.
- The P routers are route reflectors.
- EBG1 is configured with the **redistribute connected subnets** router configuration command.
- EBG2 is configured with the **neighbor next-hop-self** router configuration command.

Figure 4 Configuring Two Autonomous Systems



47866

Autonomous System 1, CE1 Configuration

```
CE1: Company
!
interface Loopback1
 ip address 1.0.0.6 255.255.255.255
!
interface Serial1/3
 description Veritas
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface Serial1/3.1 point-to-point
 description Veritas
 ip address 1.6.2.1 255.255.255.252
 frame-relay interface-dlci 22
!
router ospf 1
 network 1.0.0.0 0.255.255.255 area 0
```

Autonomous System 1, PE1 Configuration

```
PE1: Company
!
ip cef
!
ip vrf V1
 rd 1:105
 route-target export 1:100
 route-target import 1:100
!
interface Serial0/0
 description Burlington
 no ip address
 encapsulation frame-relay
 no fair-queue
```

```

        clockrate 2000000
    !
interface Serial0/0.3 point-to-point
    description Burlington
    ip vrf forwarding V1
    ip address 1.6.2.2 255.255.255.252
    frame-relay interface-dlci 22
!
interface Ethernet0/1
    description Vermont
    ip address 100.2.2.5 255.255.255.0
    tag-switching ip
!
router ospf 1
    log-adjacency-changes
    network 100.0.0.0 0.255.255.255 area 0
!
router ospf 10 vrf V1
    log-adjacency-changes
    redistribute bgp 1 metric 100 subnets
    network 1.0.0.0 0.255.255.255 area 0
!
router bgp 1
    no synchronization
    neighbor R peer-group
    neighbor R remote-as 1
    neighbor R update-source Loopback0
    neighbor 100.0.0.2 peer-group R
    no auto-summary
!
address-family ipv4 vrf V1
    redistribute ospf 10
    no auto-summary
    no synchronization
    exit-address-family
!
address-family vpnv4
    neighbor R activate
    neighbor R send-community extended
    neighbor 100.0.0.2 peer-group R
    no auto-summary
    exit-address-family

```

Autonomous System 1, P1 Configuration

```

P1: Company
!
ip cef
!
interface Loopback0
    ip address 100.0.0.2 255.255.255.255
!
interface Ethernet0/1
    description Ogunquit
    ip address 100.2.1.1 255.255.255.0
    tag-switching ip
!
interface FastEthernet2/0
    description Veritas
    ip address 100.2.2.1 255.255.255.0
    duplex auto
    speed auto
    tag-switching ip
!

```

```

router ospf 1
  log-adjacency-changes
  network 100.0.0.0 0.255.255.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  neighbor R peer-group
  neighbor R remote-as 1
  neighbor R update-source Loopback0
  neighbor R route-reflector-client
  neighbor 100.0.0.4 peer-group R
  neighbor 100.0.0.5 peer-group R
!
address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor 100.0.0.4 peer-group R
  neighbor 100.0.0.5 peer-group R
exit-address-family

```

Autonomous System 1, EBGPI Configuration

```

EBGP1: Company
!
ip cef
!
interface Loopback0
  ip address 100.0.0.4 255.255.255.255
!
interface Ethernet0/1
  description Vermont
  ip address 100.2.1.40 255.255.255.0
  tag-switching ip
!
interface ATM1/0
  description Lowell
  no ip address
  no atm scrambling cell-payload
  no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
  description Lowell
  ip address 12.0.0.1 255.255.255.252
  pvc 1/100
!
router ospf 1
  log-adjacency-changes
  redistribute connected subnets
  network 100.0.0.0 0.255.255.255 area 0
!
router bgp 1
  no synchronization
  no bgp default route-target filter
  bgp log-neighbor-changes
  neighbor R peer-group
  neighbor R remote-as 1
  neighbor R update-source Loopback0
  neighbor 12.0.0.2 remote-as 2
  neighbor 100.0.0.2 peer-group R
  no auto-summary
!
address-family vpnv4

```

```

neighbor R activate
neighbor R send-community extended
neighbor 12.0.0.2 activate
neighbor 12.0.0.2 send-community extended
neighbor 100.0.0.2 peer-group R
no auto-summary
exit-address-family

```

Autonomous System 2, EBG2 Configuration

```

EBGP2: Company
!
ip cef
!
ip vrf V1
    rd 2:103
    route-target export 1:100
    route-target import 1:100
!
interface Loopback0
    ip address 200.0.0.3 255.255.255.255
    ip router isis
!
interface Loopback1
    ip vrf forwarding V1
    ip address 1.0.0.3 255.255.255.255
!
interface Serial0/0
    description Littleton
    no ip address
    encapsulation frame-relay
    load-interval 30
    no fair-queue
    clockrate 2000000
!
interface Serial0/0.2 point-to-point
    description Littleton
    ip unnumbered Loopback0
    ip router isis
    tag-switching ip
    frame-relay interface-dlci 23
!
interface ATM1/0
    description Ogunquit
    no ip address
    atm clock INTERNAL
    no atm scrambling cell-payload
    no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
    description Ogunquit
    ip address 12.0.0.2 255.255.255.252
    pvc 1/100
!
router isis
    net 49.0002.0000.0000.0003.00
!
router bgp 2
    no synchronization
    no bgp default route-target filter
    bgp log-neighbor-changes
    neighbor 12.0.0.1 remote-as 1
    neighbor 200.0.0.8 remote-as 2
    neighbor 200.0.0.8 update-source Loopback0

```

```

        neighbor 200.0.0.8 next-hop-self
    !
    address-family ipv4 vrf V1
        redistribute connected
        no auto-summary
        no synchronization
        exit-address-family
    !
    address-family vpnv4
        neighbor 12.0.0.1 activate
        neighbor 12.0.0.1 send-community extended
        neighbor 200.0.0.8 activate
        neighbor 200.0.0.8 next-hop-self
        neighbor 200.0.0.8 send-community extended
        exit-address-family

```

Autonomous System 2, P2 Configuration

```

P2: Company
!
ip cef
!
ip vrf V1
    rd 2:108
    route-target export 1:100
    route-target import 1:100
!
interface Loopback0
    ip address 200.0.0.8 255.255.255.255
    ip router isis
!
interface Loopback1
    ip vrf forwarding V1
    ip address 1.0.0.8 255.255.255.255
!
interface FastEthernet0/0
    description Pax
    ip address 200.9.1.2 255.255.255.0
    ip router isis
    tag-switching ip
!
interface Serial5/0
    description Lowell
    no ip address
    encapsulation frame-relay
    frame-relay intf-type dce
!
interface Serial5/0.1 point-to-point
    description Lowell
    ip unnumbered Loopback0
    ip router isis
    tag-switching ip
    frame-relay interface-dlci 23
!
router isis
    net 49.0002.0000.0000.0008.00
!
router bgp 2
    no synchronization
    bgp log-neighbor-changes
    neighbor R peer-group
    neighbor R remote-as 2
    neighbor R update-source Loopback0
    neighbor R route-reflector-client

```

```

neighbor 200.0.0.3 peer-group R
neighbor 200.0.0.9 peer-group R
!
address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor 200.0.0.3 peer-group R
  neighbor 200.0.0.9 peer-group R
  exit-address-family

```

Autonomous System 2, PE2 Configuration

```

PE2: Company
!
ip cef
!
ip vrf V1
  rd 2:109
  route-target export 1:100
  route-target import 1:100
!
interface Loopback0
  ip address 200.0.0.9 255.255.255.255
  ip router isis
!
interface Loopback1
  ip vrf forwarding V1
  ip address 1.0.0.9 255.255.255.255
!
interface Serial0/0
  description Bethel
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  no fair-queue
  clockrate 2000000
!
interface Serial0/0.1 point-to-point
  description Bethel
  ip vrf forwarding V1
  ip unnumbered Loopback1
  frame-relay interface-dlci 24
!
interface FastEthernet0/1
  description Littleton
  ip address 200.9.1.1 255.255.255.0
  ip router isis
  tag-switching ip
!
router ospf 10 vrf V1
  log-adjacency-changes
  redistribute bgp 2 subnets
  network 1.0.0.0 0.255.255.255 area 0
!
router isis
  net 49.0002.0000.0000.0009.00
!

```

```

router bgp 2
  no synchronization
  bgp log-neighbor-changes
  neighbor 200.0.0.8 remote-as 2
  neighbor 200.0.0.8 update-source Loopback0
!
address-family ipv4 vrf V1
  redistribute connected
  redistribute ospf 10
  no auto-summary
  no synchronization
  exit-address-family
address-family vpnv4
  neighbor 200.0.0.8 activate
  neighbor 200.0.0.8 send-community extended
  exit-address-family

```

Autonomous System 2, CE2 Configuration

```

CE2: Company
!
interface Loopback0
  ip address 1.0.0.11 255.255.255.255
!
interface Serial0
  description Pax
  no ip address
  encapsulation frame-relay
  no fair-queue
  clockrate 2000000
!
interface Serial0.1 point-to-point
  description Pax
  ip unnumbered Loopback0
  frame-relay interface-dlci 24
!
router ospf 1
  network 1.0.0.0 0.255.255.255 area 0

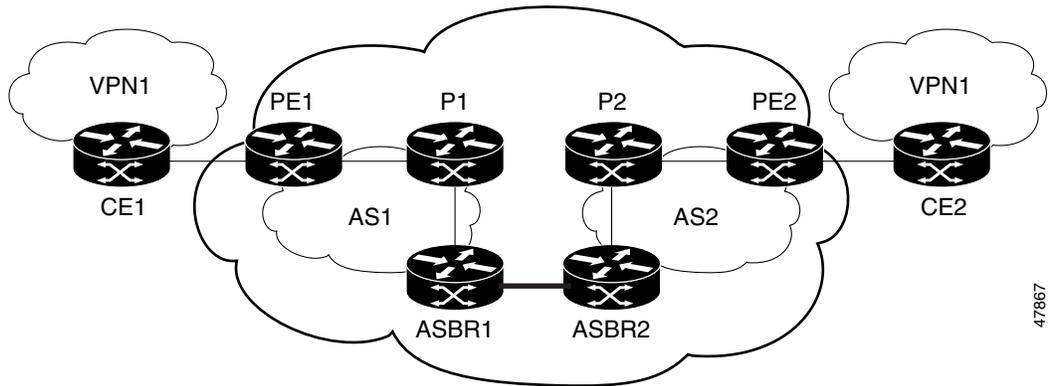
```

Configuring EBGP Routing to Exchange VPN Routes Between Autonomous Systems in a Confederation

The network topology in [Figure 5](#) shows a single ISP that is partitioning the backbone with confederations. The AS number of the provider is 100. The two autonomous systems run their own IGPs and are configured as follows:

- Autonomous system 1 (AS1) includes PE1, P1, EBGP1. The IGP is OSPF.
- Autonomous system 2 (AS2) includes PE2, P2, EBGP2. The IGP is ISIS.
- CE1 and CE2 belongs to the same VPN, which is called VPN1.
- The P routers are route reflectors.
- EBGP1 is configured with the **redistribute connected subnets** router configuration command.
- EBGP2 is configured with the **neighbor next-hop-self** router configuration command.

Figure 5 *Configuring Two Autonomous Systems in a Confederation*



47867

Autonomous System 1, CE1 Configuration

```

CE1: Company
!
interface Loopback1
    ip address 1.0.0.6 255.255.255.255
!
interface Serial1/3
    description Veritas
    no ip address
    encapsulation frame-relay
    frame-relay intf-type dce
!
interface Serial1/3.1 point-to-point
    description Veritas
    ip address 1.6.2.1 255.255.255.252
    frame-relay interface-dlci 22
!
router ospf 1
    network 1.0.0.0 0.255.255.255 area 0
    
```

Autonomous System 1, PE1 Configuration

```

PE1: Company
!
ip cef
!
ip vrf V1
    rd 1:105
    route-target export 1:100
    route-target import 1:100
!
interface Serial0/0
    description Burlington
    no ip address
    encapsulation frame-relay
    no fair-queue
    clockrate 2000000
!
interface Serial0/0.3 point-to-point
    description Burlington
    ip vrf forwarding V1
    ip address 1.6.2.2 255.255.255.252
    frame-relay interface-dlci 22
!
    
```

```

interface Ethernet0/1
  description Vermont
  ip address 100.2.2.5 255.255.255.0
  tag-switching ip
!
router ospf 1
  log-adjacency-changes
  network 100.0.0.0 0.255.255.255 area 0
!
router ospf 10 vrf V1
  log-adjacency-changes
  redistribute bgp 1 metric 100 subnets
  network 1.0.0.0 0.255.255.255 area 0
!
router bgp 1
  no synchronization
  bgp confederation identifier 100
  bgp confederation identifier 100
  neighbor R peer-group
  neighbor R remote-as 1
  neighbor R update-source Loopback0
  neighbor 100.0.0.2 peer-group R
  no auto-summary
!
address-family ipv4 vrf V1
  redistribute ospf 10
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor R activate
  neighbor R send-community extended
  neighbor 100.0.0.2 peer-group R
  no auto-summary
  exit-address-family

```

Autonomous System 1, P1 Configuration

```

P1: Company
!
ip cef
!
interface Loopback0
  ip address 100.0.0.2 255.255.255.255
!
interface Ethernet0/1
  description Ogunquit
  ip address 100.2.1.1 255.255.255.0
  tag-switching ip
!
interface FastEthernet2/0
  description Veritas
  ip address 100.2.2.1 255.255.255.0
  duplex auto
  speed auto
  tag-switching ip
!
router ospf 1
  log-adjacency-changes
  network 100.0.0.0 0.255.255.255 area 0
!
router bgp 1
  no synchronization

```

```

    bgp log-neighbor-changes
    bgp confederation identifier 100
    neighbor R peer-group
    neighbor R remote-as 1
    neighbor R update-source Loopback0
    neighbor R route-reflector-client
    neighbor 100.0.0.4 peer-group R
    neighbor 100.0.0.5 peer-group R
!
address-family vpnv4
    neighbor R activate
    neighbor R route-reflector-client
    neighbor R send-community extended
    neighbor 100.0.0.4 peer-group R
    neighbor 100.0.0.5 peer-group R
exit-address-family

```

Autonomous System 1, EBGPI Configuration

```

EBGP1: Company
!
ip cef
!
interface Loopback0
    ip address 100.0.0.4 255.255.255.255
!
interface Ethernet0/1
    description Vermont
    ip address 100.2.1.40 255.255.255.0
    tag-switching ip
!
interface ATM1/0
    description Lowell
    no ip address
    no atm scrambling cell-payload
    no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
    description Lowell
    ip address 12.0.0.1 255.255.255.252
    pvc 1/100
!
router ospf 1
    log-adjacency-changes
    redistribute connected subnets
    network 100.0.0.0 0.255.255.255 area 0
!
router bgp 1
    no synchronization
    no bgp default route-target filter
    bgp log-neighbor-changes
    bgp confederation identifier 100
    bgp confederation peers 1
    neighbor R peer-group
    neighbor R remote-as 1
    neighbor R update-source Loopback0
    neighbor 12.0.0.2 remote-as 2
    neighbor 12.0.0.2 next-hop-self
    neighbor 100.0.0.2 peer-group R
    no auto-summary
!
address-family vpnv4
    neighbor R activate
    neighbor R send-community extended

```

```

neighbor 12.0.0.2 activate
neighbor 12.0.0.2 next-hop-self
neighbor 12.0.0.2 send-community extended
neighbor 100.0.0.2 peer-group R
no auto-summary
exit-address-family

```

Autonomous System 2, EBG2 Configuration

```

EBGP2: Company
!
ip cef
!
ip vrf V1
    rd 2:103
    route-target export 1:100
    route-target import 1:100
!
interface Loopback0
    ip address 200.0.0.3 255.255.255.255
    ip router isis
!
interface Loopback1
    ip vrf forwarding V1
    ip address 1.0.0.3 255.255.255.255
!
interface Serial0/0
    description Littleton
    no ip address
    encapsulation frame-relay
    load-interval 30
    no fair-queue
    clockrate 2000000
!
interface Serial0/0.2 point-to-point
    description Littleton
    ip unnumbered Loopback0
    ip router isis
    tag-switching ip
    frame-relay interface-dlci 23
!
interface ATM1/0
    description Ogunquit
    no ip address
    atm clock INTERNAL
    no atm scrambling cell-payload
    no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
    description Ogunquit
    ip address 12.0.0.2 255.255.255.252
    pvc 1/100
!
router isis
    net 49.0002.0000.0000.0003.00
!
router bgp 2
    no synchronization
    no bgp default route-target filter
    bgp log-neighbor-changes
    bgp confederation identifier 100
    bgp confederation peers 1
    neighbor 12.0.0.1 remote-as 1
    neighbor 12.0.0.1 next-hop-self

```

```

neighbor 200.0.0.8 remote-as 2
neighbor 200.0.0.8 update-source Loopback0
neighbor 200.0.0.8 next-hop-self
!
address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor 12.0.0.1 activate
  neighbor 12.0.0.1 next-hop-self
  neighbor 12.0.0.1 send-community extended
  neighbor 200.0.0.8 activate
  neighbor 200.0.0.8 next-hop-self
  neighbor 200.0.0.8 send-community extended
  exit-address-family

```

Autonomous System 2, P2 Configuration

```

P2: Company
!
ip cef
!
ip vrf V1
  rd 2:108
  route-target export 1:100
  route-target import 1:100
!
interface Loopback0
  ip address 200.0.0.8 255.255.255.255
  ip router isis
!
interface Loopback1
  ip vrf forwarding V1
  ip address 1.0.0.8 255.255.255.255
!
interface FastEthernet0/0
  description Pax
  ip address 200.9.1.2 255.255.255.0
  ip router isis
  tag-switching ip
!
interface Serial5/0
  description Lowell
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
!
interface Serial5/0.1 point-to-point
  description Lowell
  ip unnumbered Loopback0
  ip router isis
  tag-switching ip
  frame-relay interface-dlci 23
!
router isis
  net 49.0002.0000.0000.0008.00
!
router bgp 2
  no synchronization
  bgp log-neighbor-changes
  bgp confederation identifier 100

```

```

neighbor R peer-group
neighbor R remote-as 2
neighbor R update-source Loopback0
neighbor R route-reflector-client
neighbor 200.0.0.3 peer-group R
neighbor 200.0.0.9 peer-group R
!
address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor 200.0.0.3 peer-group R
  neighbor 200.0.0.9 peer-group R
  exit-address-family

```

Autonomous System 2, PE2 Configuration

```

PE2: Company
!
ip cef
!
ip vrf V1
  rd 2:109
  route-target export 1:100
  route-target import 1:100
!
interface Loopback0
  ip address 200.0.0.9 255.255.255.255
  ip router isis
!
interface Loopback1
  ip vrf forwarding V1
  ip address 1.0.0.9 255.255.255.255
!
interface Serial0/0
  description Bethel
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  no fair-queue
  clockrate 2000000
!
interface Serial0/0.1 point-to-point
  description Bethel
  ip vrf forwarding V1
  ip unnumbered Loopback1
  frame-relay interface-dlci 24
!
interface FastEthernet0/1
  description Littleton
  ip address 200.9.1.1 255.255.255.0
  ip router isis
  tag-switching ip
!
router ospf 10 vrf V1
  log-adjacency-changes
  redistribute bgp 2 subnets
  network 1.0.0.0 0.255.255.255 area 0

```

```

!
router isis
    net 49.0002.0000.0000.0009.00
!
router bgp 2
    no synchronization
    bgp log-neighbor-changes
    bgp confederation identifier 100
    neighbor 200.0.0.8 remote-as 2
    neighbor 200.0.0.8 update-source Loopback0
!
address-family ipv4 vrf V1
    redistribute connected
    redistribute ospf 10
    no auto-summary
    no synchronization
    exit-address-family
address-family vpnv4
    neighbor 200.0.0.8 activate
    neighbor 200.0.0.8 send-community extended
    exit-address-family

```

Autonomous System 2, CE2 Configuration

```

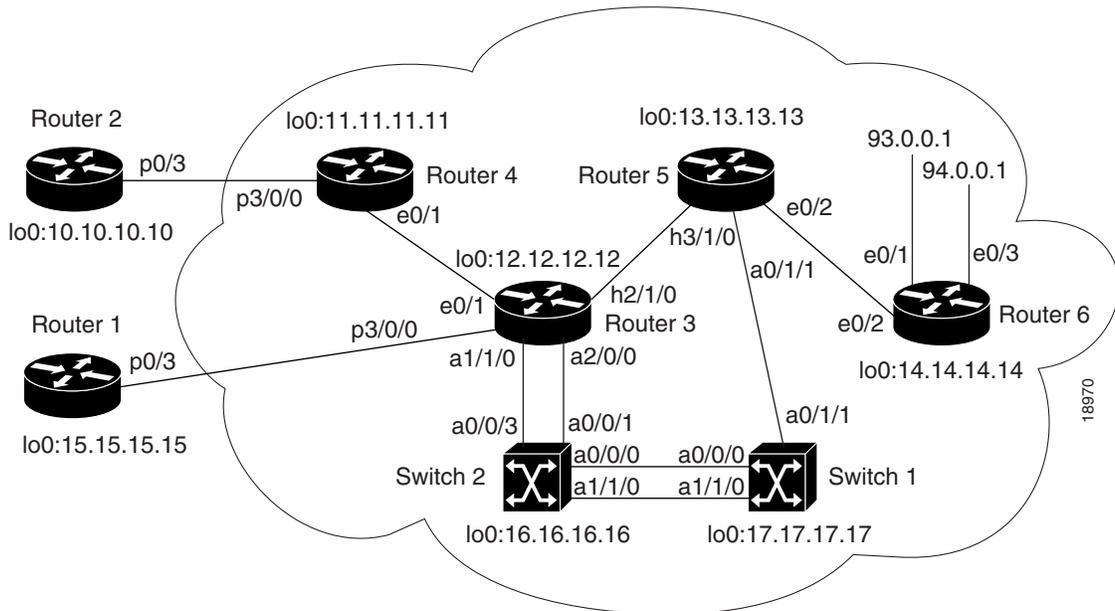
CE2: Company
!
interface Loopback0
    ip address 1.0.0.11 255.255.255.255
!
interface Serial0
    description Pax
    no ip address
    encapsulation frame-relay
    no fair-queue
    clockrate 2000000
!
interface Serial0.1 point-to-point
    description Pax
    ip unnumbered Loopback0
    frame-relay interface-dlci 24
!
router ospf 1
    network 1.0.0.0 0.255.255.255 area 0

```

Implementing MPLS QoS Example

Figure 6 illustrates a sample MPLS topology that implements the MPLS QoS feature. The following sections contain the configuration commands entered on Routers R1 to R6 and on Switches 1 and 2 included in this figure.

Figure 6 Sample MPLS Topology Implementing QoS



Configuring CEF Example

The following configuration commands enable CEF. CEF switching is a prerequisite for the MPLS feature and must be running on all routers in the network:

```
ip cef distributed
tag-switching ip
!
```

Running IP on Router 2 Example

The following commands enable IP routing on Router 2. All routers must have IP enabled:



Note

Router 2 is not part of the MPLS network.

```
!
ip routing
!
hostname R2
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface POS0/3
 ip unnumbered Loopback0
 crc 16
 clock source internal
!
router ospf 100
 network 10.0.0.0 0.255.255.255 area 100
!
```

Running IP on Router 1 Example

The following commands enable IP routing on Router 1:



Note

Router 1 is not part of the MPLS network.

```
ip routing
!
hostname R1
!
interface Loopback0
 ip address 15.15.15.15 255.255.255.255
!
interface POS0/3
 ip unnumbered Loopback0
 crc 16
 clock source internal
!
router ospf 100
 network 15.0.0.0 0.255.255.255 area 100
```

Running MPLS on Router 4 Example

Router 4 is a label edge router. CEF and the MPLS feature must be enabled on this router. CAR is also configured on Router 4 on interface POS3/0/0 (see the following section on configuring CAR).

```
!
hostname R4
!
ip routing
tag-switching ip
tag-switching advertise-tags
!
ip cef distributed
!
interface Loopback0
 ip address 11.11.11.11 255.255.255.255
!
interface Ethernet0/1
 ip address 90.0.0.1 255.0.0.0
tag-switching ip
!
```

Configuring CAR Example

Lines 3 and 4 of the following sample configuration contain the CAR rate policies. Line 3 sets the committed information rate (CIR) at 155,000,000 bits and the normal burst/maximum burst size at 200,000/800,000 bytes. The conform action (action to take on packets) sets the IP precedence and sends the packets that conform to the rate limit. The exceed action sets the IP precedence and sends the packets when the packets exceed the rate limit.

```
!
interface POS3/0/0
 ip unnumbered Loopback0
 rate-limit input 155000000 200000 800000 conform-action set-prec-transmit 5
 exceed-action set-prec-transmit 1
 ip route-cache distributed
!
router ospf 100
```

```
network 11.0.0.0 0.255.255.255 area 100
network 90.0.0.0 0.255.255.255 area 100
```

Running MPLS on Router 3 Example

Router 3 is running MPLS. CEF and the MPLS feature must be enabled on this router. Router 3 contains interfaces that are configured for WRED, multi-VC, per-VC WRED, WFQ, and CAR. The following sections contain these sample configurations:

```
!
hostname R3
!
ip cef distributed
!
interface Loopback0
 ip address 12.12.12.12 255.255.255.255
!
interface Ethernet0/1
 ip address 90.0.0.2 255.0.0.0
tag-switching ip
```

Configuring Point-to-Point WRED Example

The following commands configure WRED on an ATM interface. In this example, the commands refer to a PA-A1 port adapter.

```
!
interface ATM1/1/0
ip route-cache distributed
 atm clock INTERNAL
 random-detect
!
```

Configuring an Interface for Multi-VC Mode Example

The following commands configure interface ATM1/1/0 for multi-VC mode. In this example, the commands refer to a PA-A1 port adapter.

```
!
interface ATM1/1/0.1 tag-switching
 ip unnumbered Loopback0
tag-switching atm multi-vc
 tag-switching ip
!
```

Configuring WRED and Multi-VC Mode on a PA-A3 Port-Adapter Interface Example

The commands to configure a PA-A3 port adapter differ slightly from the commands to configure a PA-A1 port adapter as shown previously.

On an PA-A3 port-adapter interface, distributed WRED (DWRED) is supported only per-VC, not per-interface.

To configure a PA-A3 port adapter, enter the following commands:

```
!
interface ATM1/1/0
ip route-cache distributed
 atm clock INTERNAL
!
```

```
interface ATM 1/1/0.1 tag-switching
ip unnumbered Loopback0
tag-switching multi-vc
tag-switching random detect attach groupname
!
```

Configuring Per-VC WRED Example

The following commands configure per-VC WRED on a PA-A3 port adapter only:



Note

The PA-A1 port adapter does not support the per-VC WRED drop mechanism.

```
!interface ATM2/0/0
no ip address
ip route-cache distributed

interface ATM2/0/0.1 point-to-point
ip unnumbered Loopback0
no ip directed-broadcast
pvc 10/100
random-detect
encapsulation aal5snap
exit
!
tag-switching ip
```

Configuring WRED and WFQ Example

Lines 5 and 6 of the following sample configuration contain the commands for configuring WRED and WFQ on interface Hssi2/1/0:

```
!
interface Hssi2/1/0
ip address 91.0.0.1 255.0.0.0
ip route-cache distributed
tag-switching ip
random-detect
fair queue tos
hssi internal-clock
!
```

Configuring CAR Example

Lines 3 and 4 of the following sample configuration contain the CAR rate policies. Line 3 sets the CIR at 155,000,000 bits and the normal burst/maximum burst size at 200,000/800,000 bytes. The conform action (action to take on packets) sets the IP precedence and sends the packets that conform to the rate limit. The exceed action sets the IP precedence and sends the packets when the packets exceed the rate limit.

```
!
interface POS3/0/0
ip unnumbered Loopback0
rate-limit input 155000000 2000000 8000000 conform-action set-prec-transmit 2
exceed-action set-prec-transmit 2
ip route-cache distributed
!
router ospf 100
network 12.0.0.0 0.255.255.255 area 100
```

```

network 90.0.0.0 0.255.255.255 area 100
network 91.0.0.0 0.255.255.255 area 100
!
ip route 93.0.0.0 255.0.0.0 Hssi2/1/0 91.0.0.2
!
```

Running MPLS on Router 5 Example

Router 5 is running the MPLS feature. CEF and MPLS must be enabled on this router. Router 5 has also been configured to create an ATM subinterface in multi-VC mode and to create a PVC on a point-to-point subinterface. The sections that follow contain these sample configurations.

```

!
hostname R5
!
ip cef distributed
!
interface Loopback0
 ip address 13.13.13.13 255.255.255.255
!
interface Ethernet0/2
 ip address 92.0.0.1 255.0.0.0
 tag-switching ip
```

Configuring an ATM Interface Example

The following commands create an ATM interface:

```

!
interface ATM1/0/0
 no ip address
 ip route-cache distributed
 atm clock INTERNAL
!
```

Configuring an ATM MPLS Subinterface in Multi-VC Mode Example

The following commands create an MPLS subinterface in multi-VC mode:

```

!
interface ATM1/0/0.1 tag-switching
 ip unnumbered Loopback0
 tag-switching atm multi-vc
 tag-switching ip
!
```

Configuring a PVC on Point-to-Point Subinterface Example

The following commands create a PVC on a point-to-point subinterface (interface ATM1/0/0.2).

```

!
interface ATM1/0/0.2 point-to-point
 ip unnumbered Loopback0
 pvc 10/100
 random-detect
 encapsulation aal5snap
 exit
!
 tag-switching ip
!
interface Hssi3/0
 ip address 91.0.0.2 255.0.0.0
```

```

tag-switching ip
 hssi internal-clock
!
router ospf 100
 network 13.0.0.0 0.255.255.255 area 100
 network 91.0.0.0 0.255.255.255 area 100
 network 92.0.0.0 0.255.255.255 area 100
!

```

Running MPLS on Router 6 Example

Router 6 is running the MPLS feature. CEF and MPLS must be enabled on this router. The following commands configure MPLS on an ethernet interface:

```

!
hostname R6
!
ip cef distributed
!
interface Loopback0
 ip address 14.14.14.14 255.255.255.255
!
interface Ethernet0/1
 ip address 93.0.0.1 255.0.0.0
tag-switching ip
!
interface Ethernet0/2
 ip address 92.0.0.2 255.0.0.0
 tag-switching ip
!
interface Ethernet0/3
 ip address 94.0.0.1 255.0.0.0
 tag-switching ip
!
router ospf 100
 network 14.0.0.0 0.255.255.255 area 100
 network 92.0.0.0 0.255.255.255 area 100
 network 93.0.0.0 0.255.255.255 area 100
 network 94.0.0.0 0.255.255.255 area 100
!

```

Configuring ATM Switch 2 Example

Switch 2 is configured for MPLS and creates an ATM Forum PVC. The following commands configure MPLS on ATM switch2:

```

!
hostname S2
!
interface Loopback0
 ip address 16.16.16.16 255.255.255.255
!
interface ATM0/0/0
 ip unnumbered Loopback0
tag-switching ip
!
interface ATM0/0/1
 ip unnumbered Loopback0
 tag-switching ip
atm pvc 10 100 interface ATM0/0/0 10 100

```

```

interface ATM0/0/2
  no ip address
  no ip directed-broadcast
  !
interface ATM0/0/3
  ip unnumbered Loopback0
  tag-switching ip
  !
interface ATM1/1/0
  ip unnumbered Loopback0
  tag-switching ip
  !
router ospf 100
  network 16.0.0.0 0.255.255.255 area 100
  !

```

Configuring ATM Switch 1 Example

Switch 1 is configured to create an ATM Forum PVC. The following commands configure MPLS on ATM switch1:

```

!
hostname S1
!
interface Loopback0
  ip address 17.17.17.17 255.255.255.255
!
interface ATM0/0/0
  ip unnumbered Loopback0
  tag-switching ip
!

```

Configuring Label VCs and an ATM Forum PVC Example

Line 3 of the following sample configuration contains the configuration command for an ATM Forum PVC:

```

!
interface ATM0/1/1
  ip unnumbered Loopback0
  atm pvc 10 100 interface ATM0/0/0 10 100
  tag-switching ip
!
interface ATM1/1/0
  ip unnumbered Loopback0
  tag-switching ip
!
router ospf 100
  network 17.0.0.0 0.255.255.255 area 100
!

```

Configuring an MPLS LSC Examples

The following sections present the following MPLS LSC configuration examples:

- [Configuring ATM-LSRs Example](#)
- [Configuring Multi-VCs Example](#)
- [Configuring ATM-LSRs with a Cisco 6400 NRP Operating as LSC Example](#)

- [Configuring ATM LSRs Through ATM Network Using Cisco 7200 LSCs Implementing Virtual Trunking Example](#)
- [Configuring ATM LSRs Through ATM Network Using Cisco 6400 NRP LSCs Implementing Virtual Trunking Example](#)
- [Configuring LSC Hot Redundancy Example](#)
- [Configuring LSC Warm Standby Redundancy Example](#)
- [Configuring an Interface Using Two VSI Partitions Example](#)
- [Using an Access List to Control the Creation of Headend VCs](#)

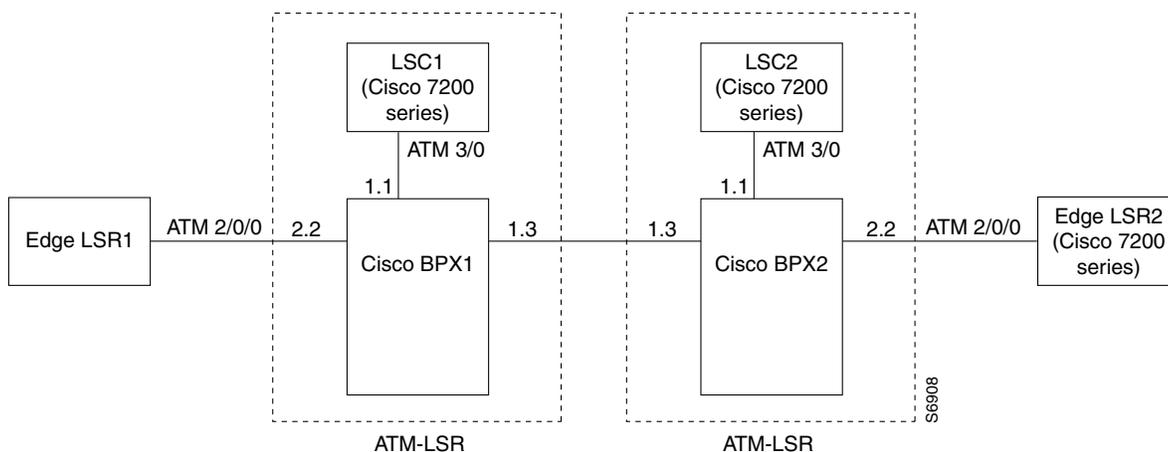
Configuring ATM-LSRs Example

The network topology shown in [Figure 7](#) incorporates two ATM-LSRs in an MPLS network. This topology includes two LSCs (Cisco 7200 routers), two BPX service nodes, and two edge LSRs (Cisco 7500 routers).

For the IGX, use the following commands:

```
extended-port atm1/0 descriptor 0.x.x.0
tag-control-protocol vsi slaves 32 id x
```

Figure 7 ATM-LSR Network Configuration Example



Based on [Figure 7](#), the following configuration examples are provided:

- [LSC1 Configuration](#)
- [BPX1 and BPX2 Configuration](#)
- [LSC2 Configuration](#)
- [Edge LSR1 Configuration](#)
- [Edge LSR2 Configuration](#)

LSC1 Configuration

```
7200 LSC1:
ip cef
!
interface loopback0
ip address 192.103.210.5 255.255.255.255
```

```

!
interface ATM3/0
  no ip address
  tag-control-protocol vsi
!
interface XTagATM13
  extended-port ATM3/0 bpx 1.3
  ip unnumbered loopback0
  tag-switching atm vpi 2-15
  tag-switching ip
!
interface XTagATM22
  extended-port ATM3/0 bpx 2.2
  ip unnumbered loopback0
  tag-switching atm vpi 2-5
  tag-switching ip

```

BPX1 and BPX2 Configuration

BPX1 and BPX2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3
cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```



Note

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for example, XTagATM11).

LSC2 Configuration

```

7200 LSC2:
  ip cef
  !
  interface loopback0
    ip address 142.2.143.22 255.255.255.255
  !
  interface ATM3/0
    no ip address
    tag-control-protocol vsi
  !
  interface XTagATM13
    extended-port ATM3/0 bpx 1.3
    ip unnumbered loopback0
    tag-switching atm vpi 2-15
    tag-switching ip
  !
  interface XTagATM22
    extended-port ATM3/0 bpx 2.2
    ip unnumbered loopback0
    tag-switching atm vpi 2-5
    tag-switching ip
  !

```

Edge LSR1 Configuration

```

7500 LSR1:
  ip cef distributed
  !
  interface loopback 0

```

```

ip address 142.6.132.2 255.255.255.255
!
interface ATM2/0/0
    no ip address
!
interface ATM2/0/0.5 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching ip

```

Edge LSR2 Configuration

```

7200 LSR2:
    ip cef
    interface loopback 0
        ip address 142.6.142.2 255.255.255.255
    !
    interface ATM2/0
        no ip address
    !
    interface ATM2/0.9 tag-switching
        ip unnumbered loopback 0
        tag-switching atm vpi 2-5
        tag-switching ip

```

Configuring Multi-VCs Example

When you configure multi-VC support, four label VCs for each destination are created by default, as follows:

- Standard (for class 0 and class 4 traffic)
- Available (for class 1 and class 5 traffic)
- Premium (for class 2 and class 6 traffic)
- Control (for class 3 and class 7 traffic)

This section provides examples for the following configurations, based on the sample network configuration shown earlier in [Figure 7](#):

- [LSC1 Configuration](#)
- [BPX1 and BPX2 Configuration](#)
- [LSC2 Configuration](#)
- [Edge LSR1 Configuration](#)
- [Edge LSR2 Configuration](#)



Note

The IGX series ATM switches do not support QoS.

LSC1 Configuration

```

7200 LSC1:
    ip cef
    !
    interface loopback0
        ip address 192.103.210.5 255.255.255.255
    !
    interface ATM3/0

```

```

no ip address
    tag-control-protocol vsi
!
interface XTagATM13
    ip unnumbered loopback 0
    extended-port ATM3/0 bpx 1.3
    tag-switching atm vpi 2-15
    tag-switching atm cos available 25
    tag-switching atm cos standard 25
    tag-switching atm cos premium 25
    tag-switching atm cos control 25
    tag-switching ip
!
interface XTagATM23
    ip unnumbered loopback 0
    extended-port ATM3/0 bpx 2.2
    tag-switching atm vpi 2-5
    tag-switching atm cos available 20
    tag-switching atm cos standard 30
    tag-switching atm cos premium 25
    tag-switching atm cos control 25
    tag-switching ip

```

BPX1 and BPX2 Configuration

BPX1 and BPX2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3
cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```

LSC2 Configuration

7200 LSC2:

```

ip cef
!
interface loopback0
    ip address 142.2.143.22 255.255.255.255
!
    interface ATM3/0
        no ip address
        tag-control-protocol vsi
!
interface XTagATM13
    ip unnumbered loopback 0
    extended-port ATM3/0 bpx 1.3
    tag-switching atm vpi 2-15
    tag-switching atm cos available 25
    tag-switching atm cos standard 25
    tag-switching atm cos premium 25
    tag-switching atm cos control 25
    tag-switching ip
!
interface XTagATM23
    ip unnumbered loopback 0
    extended-port ATM3/0 bpx 2.2
    tag-switching atm vpi 2-5
    tag-switching atm cos available 20
    tag-switching atm cos standard 30
    tag-switching atm cos premium 25
    tag-switching atm cos control 25

```

```
tag-switching ip
```

Edge LSR1 Configuration

```
7500 LSR1:
  ip cef distributed
  interface loopback 0
  ip address 142.6.132.2 255.255.255.255
  !
  interface ATM2/0/0
    no ip address
  !
  interface ATM2/0/0.5 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching atm multi-vc
    tag-switching ip
```

Edge LSR2 Configuration

```
7200 LSR2:
  ip cef
  interface loopback 0
  ip address 142.2.142.2 255.255.255.255
  !
  interface ATM2/0
    no ip address
  !
  interface ATM2/0.9 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching atm multi-vc
    tag-switching ip
```

QoS Support

If LSR1 supports QoS, but LSR2 does not, LSR1 makes VC requests for the following default classes:

- Control=QoS3
- Standard=QoS1

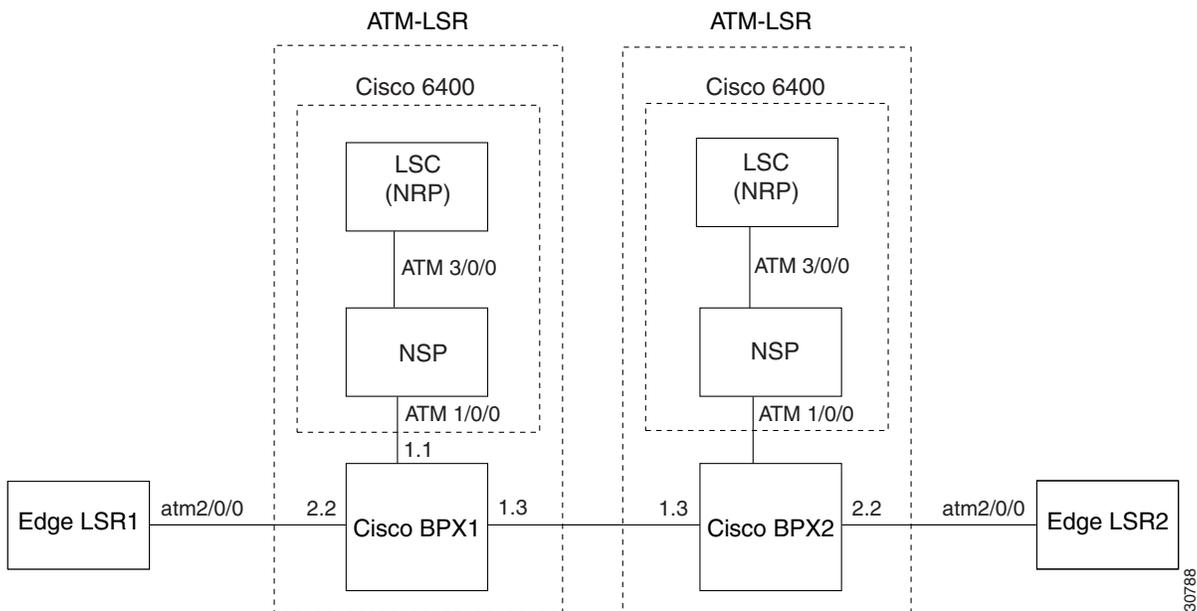
LSR2 ignores the call field in the request and allocates two UBR label VCs.

If LSR1 supports QoS, but LSR2 does not, LSR2 receives the request to create multiple label VCs, but by default, creates class 0 only (UBR).

Configuring ATM-LSRs with a Cisco 6400 NRP Operating as LSC Example

When you use the NRP as an MPLS LSC in the Cisco 6400 UAC, you must configure the NSP to provide connectivity between the NRP and the Cisco BPX switch. When configured in this way (as shown in [Figure 8](#)), the NRP is connected to the NSP by means of the internal interface ATM3/0/0, while external connectivity from the Cisco 6400 UAC to the Cisco BPX switch is provided by means of the external interface ATM1/0/0 from the NSP.

Figure 8 Cisco 6400 UAC NRP Operating As an LSC



Based on [Figure 8](#), the following configuration examples are provided:

- [6400 UAC NSP Configuration](#)
- [6400 UAC NRP LSC1 Configuration](#)
- [BPX1 and BPX2 Configuration](#)
- [6400 UAC NRP LSC2 Configuration](#)
- [Edge LSR1 Configuration](#)
- [Edge LSR2 Configuration](#)

6400 UAC NSP Configuration

```
6400 NSP:
!
interface ATM3/0/0
 atm pvp 0 interface ATM1/0/0 0
 atm pvp 2 interface ATM1/0/0 2
 atm pvp 3 interface ATM1/0/0 3
 atm pvp 4 interface ATM1/0/0 4
 atm pvp 5 interface ATM1/0/0 5
 atm pvp 6 interface ATM1/0/0 6
 atm pvp 7 interface ATM1/0/0 7
 atm pvp 8 interface ATM1/0/0 8
 atm pvp 9 interface ATM1/0/0 9
 atm pvp 10 interface ATM1/0/0 10
 atm pvp 11 interface ATM1/0/0 11
 atm pvp 12 interface ATM1/0/0 12
 atm pvp 13 interface ATM1/0/0 13
 atm pvp 14 interface ATM1/0/0 14
 atm pvp 15 interface ATM1/0/0 15
```

**Note**

Instead of configuring multiple PVCs, you can also configure PVP 0 by deleting all well-known VCs. For example, you can use the **atm manual-well-known-vc delete** interface command on both interfaces and then configure PVP 0, as follows:

atm pvp 0 interface ATM1/0/0 0**6400 UAC NRP LSC1 Configuration**

```
ip cef
!
interface Loopback0
 ip address 142.2.143.22 255.255.255.255
!
interface ATM0/0/0
 no ip address
 tag-control-protocol vsi
!
interface XTagATM13
 ip unnumbered Loopback0
 extended-port ATM0/0/0 bpx 1.3
 tag-switching atm vpi 2-15
 tag-switching ip
!
interface XTagATM22
 ip unnumbered Loopback0
 extended-port ATM0/0/0 bpx 2.2
 tag-switching atm vpi 2-5
 tag-switching ip
!
tag-switching atm disable-headend-vc
```

BPX1 and BPX2 Configuration

```
BPX1 and BPX2:
 uptrk 1.1
 addshelf 1.1 v 1 1
 cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
 uptrk 1.3
 cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
 uptrk 2.2
 cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000
```

**Note**

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for example, XTagATM11).

6400 UAC NRP LSC2 Configuration

```
ip cef
!
interface Loopback0
 ip address 192.103.210.5 255.255.255.255
!
interface ATM0/0/0
 no ip address
 tag-control-protocol vsi
!
interface XTagATM13
 ip unnumbered Loopback0
 extended-port ATM0/0/0 bpx 1.3
 tag-switching atm vpi 2-15
```

```

tag-switching ip
!
interface XTagATM22
 ip unnumbered Loopback0
 extended-port ATM0/0/0 bpx 2.2
 tag-switching atm vpi 2-5
 tag-switching ip
!
tag-switching atm disable-headend-vc

```

Edge LSR1 Configuration

```

7500 LSR1:
 ip cef distributed
 !
 interface loopback 0
 ip address 142.6.132.2 255.255.255.255
 !
 interface ATM2/0/0
 no ip address
 !
 interface ATM2/0/0.22 tag-switching
 ip unnumbered loopback 0
 tag-switching atm vpi 2-5
 tag-switching ip

```

Edge LSR2 Configuration

```

7500 LSR2:
 ip cef distributed
 !
 interface loopback 0
 ip address 142.6.142.2 255.255.255.255
 !
 interface ATM2/0/0
 no ip address
 !
 interface ATM2/0/0.22 tag-switching
 unnumbered loopback 0
 tag-switching atm vpi 2-5
 tag-switching ip

```

Configuring ATM LSRs Through ATM Network Using Cisco 7200 LSCs Implementing Virtual Trunking Example

The network topology shown in [Figure 9](#) incorporates two ATM-LSRs using virtual trunking to create an MPLS network through a private ATM Network. This topology includes the following:

- Two LSCs (Cisco 7200 routers)
- Two BPX service nodes
- Two edge LSRs (Cisco 7500 and 7200 routers)

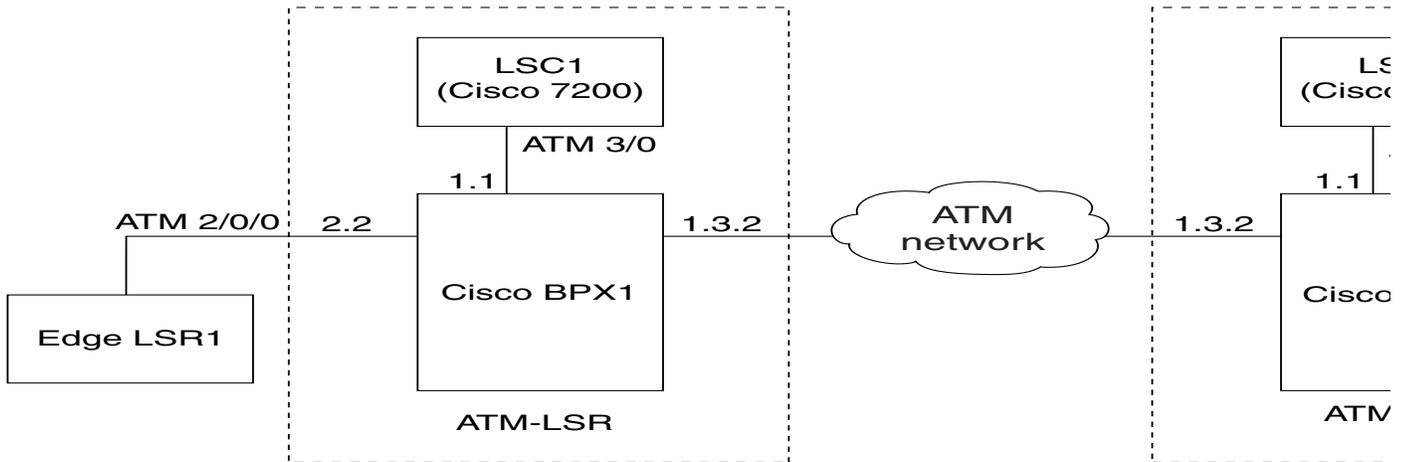
For the IGX, use the following commands:

```

extended-port atm1/0 descriptor 0.x.x.0
tag-control-protocol vsi slaves 32 id x

```

Figure 9 ATM-LSR Virtual Trunking Through an ATM Network



Based on [Figure 9](#), the following configuration examples are provided:

- [LSC1 Implementing Virtual Trunking Configuration](#)
- [BPX1 and BPX2 Configuration](#)
- [LSC2 Implementing Virtual Trunking Configuration](#)
- [Edge LSR1 Configuration](#)
- [Edge LSR2 Configuration](#)

LSC1 Implementing Virtual Trunking Configuration

```
7200 LSC1:
ip cef
!
interface loopback0
ip address 192.103.210.5 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
!
interface XTagATM132
extended-port ATM3/0 bpx 1.3.2
ip unnumbered loopback0
tag-switching atm vp-tunnel 2
tag-switching ip
!
interface XTagATM22
extended-port ATM3/0 bpx 2.2
ip unnumbered loopback0
tag-switching atm vpi 2-5
tag-switching ip
```

BPX1 and BPX2 Configuration

```
BPX1 and BPX2:
uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3.2
```

```

cnftrk 1.3.2 100000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,RT-VBR N TERRESTRIAL 10
  0 N N Y Y Y CBR 2
cnfrsrc 1.3.2 256 252207 y 1 e 512 6144 2 2 26000 100000
  uptrk 2.2
  cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```

**Note**

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XtagATM port for the VSI partition (for example, XtagATM11).

LSC2 Implementing Virtual Trunking Configuration

```

7200 LSC2:
  ip cef
  !
  interface loopback0
    ip address 142.2.143.22 255.255.255.255
    !
  interface ATM3/0
    no ip address
    tag-control-protocol vsi
    !
  interface XTagATM132
    extended-port ATM3/0 bpx 1.3.2
    ip unnumbered loopback0
    tag-switching atm vp-tunnel 2
    tag-switching ip
    !
  interface XTagATM22
    extended-port ATM3/0 bpx 2.2
    ip unnumbered loopback0
    tag-switching atm vpi 2-5
    tag-switching ip

```

Edge LSR1 Configuration

```

7500 LSR1:
  ip cef distributed
  interface loopback 0
    ip address 142.6.132.2 255.255.255.255
    !
  interface ATM2/0/0
    no ip address
    !
  interface ATM2/0/0.22 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching ip

```

Edge LSR2 Configuration

```

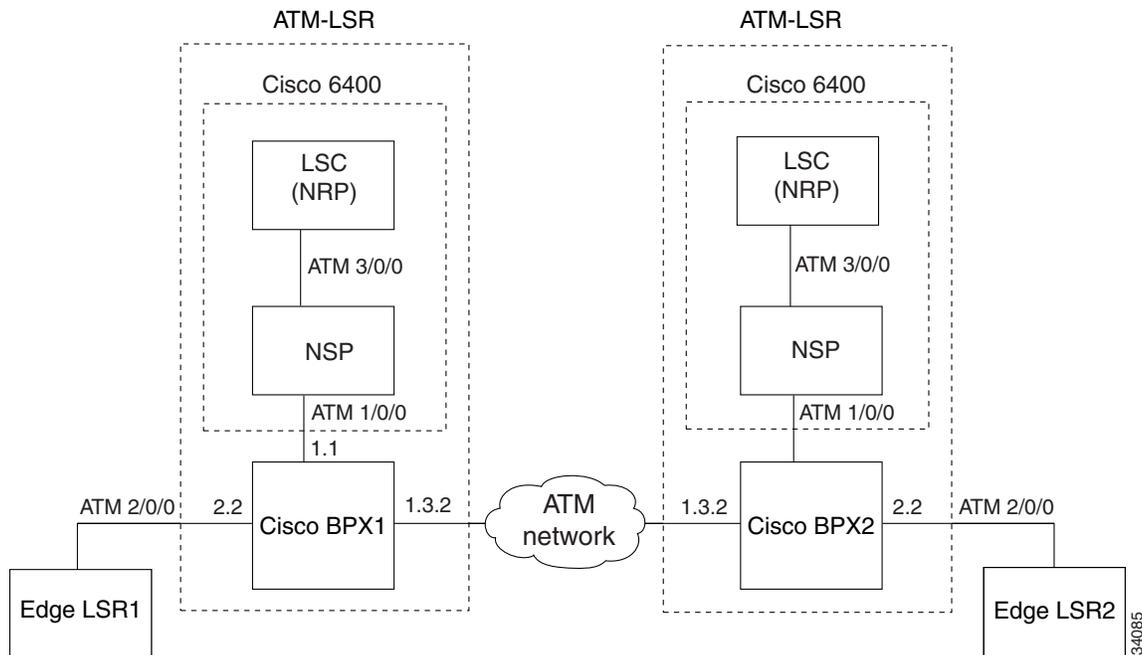
7200 LSR2:
  ip cef
  interface loopback 0
    ip address 142.6.142.2 255.255.255.255
    !
  interface ATM2/0
    no ip address
    !
  interface ATM2/0.22 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching ip

```

Configuring ATM LSRs Through ATM Network Using Cisco 6400 NRP LSCs Implementing Virtual Trunking Example

The network topology shown in [Figure 10](#) incorporates two ATM-LSRs using virtual trunking to create an MPLS network through a private ATM network. This topology includes two LSCs (Cisco 6400 UAC NRP routers), two BPX service nodes, and two edge LSRs (Cisco 7500 and 7200 routers).

Figure 10 Cisco 6400 NRP Operating as LSC Implementing Virtual Trunking



Based on [Figure 10](#), the following configuration examples are provided:

- [6400 UAC NSP Configuration](#)
- [6400 UAC NRP LSC1 Implementing Virtual Trunking Configuration](#)
- [BPX1 and BPX2 Configuration](#)
- [6400 UAC NRP LSC2 Implementing Virtual Trunking Configuration](#)
- [Edge LSR1 Configuration](#)
- [Edge LSR2 Configuration](#)

6400 UAC NSP Configuration

```
6400 NSP:
!
interface ATM3/0/0
  atm pvp 0 interface ATM1/0/0 0
  atm pvp 2 interface ATM1/0/0 2
  atm pvp 3 interface ATM1/0/0 3
  atm pvp 4 interface ATM1/0/0 4
  atm pvp 5 interface ATM1/0/0 5
  atm pvp 6 interface ATM1/0/0 6
  atm pvp 7 interface ATM1/0/0 7
  atm pvp 8 interface ATM1/0/0 8
  atm pvp 9 interface ATM1/0/0 9
```

```

atm pvp 10 interface ATM1/0/0 10
atm pvp 11 interface ATM1/0/0 11
atm pvp 12 interface ATM1/0/0 12
atm pvp 13 interface ATM1/0/0 13
atm pvp 14 interface ATM1/0/0 14
atm pvp 15 interface ATM1/0/0 15

```

**Note**

Instead of configuring multiple PVCs, you can also configure PVP 0 by deleting all well-known VCs. For example, you can use the **atm manual-well-known-vc delete** interface command on both interfaces and then configure PVP 0, as follows:

atm pvp 0 interface ATM1/0/0 0

6400 UAC NRP LSC1 Implementing Virtual Trunking Configuration

```

ip cef
!
interface Loopback0
 ip address 142.2.143.22 255.255.255.255
!
interface ATM0/0/0
 no ip address
tag-control-protocol vsi
!
interface XTagATM132
 ip unnumbered Loopback0
 extended-port ATM0/0/0 bpx 1.3.2
 tag-switching atm vp-tunnel 2
 tag-switching ip
!
interface XTagATM22
 ip unnumbered Loopback0
 extended-port ATM0/0/0 bpx 2.2
 tag-switching atm vpi 2-5
 tag-switching ip
!
tag-switching atm disable-headend-vc
BPX1 and BPX2 Configuration
BPX1 and BPX2:
 uptrk 1.1
  addshelf 1.1 v 1 1
  cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
 uptrk 1.3.2
 cnftrk 1.3.2 100000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,RT-VBR N TERRESTRIAL 10
  0 N N Y Y Y CBR 2
 cnfrsrc 1.3.2 256 252207 y 1 e 512 6144 2 2 26000 100000
 uptrk 2.2
  cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```

**Note**

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XtagATM port for the VSI partition (for example, XtagATM11).

6400 UAC NRP LSC2 Implementing Virtual Trunking Configuration

```

ip cef
!
interface Loopback0
 ip address 192.103.210.5 255.255.255.255
!
interface ATM0/0/0

```

```

        no ip address
        tag-control-protocol vsi
    !
interface XTagATM132
    ip unnumbered Loopback0
    extended-port ATM0/0/0 bpx 1.3.2
    tag-switching atm vp-tunnel 2
    tag-switching ip
!
interface XTagATM22
    ip unnumbered Loopback0
    extended-port ATM0/0/0 bpx 2.2
    tag-switching atm vpi 2-5
    tag-switching ip
!
tag-switching atm disable-headend-vc

```

Edge LSR1 Configuration

```

7500 LSR1:
    ip cef distributed
    !
interface loopback 0
    ip address 142.6.132.2 255.255.255.255
    !
interface ATM2/0/0
    no ip address
    !
interface ATM2/0/0.22 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching ip

```

Edge LSR2 Configuration

```

7500 LSR2:
    ip cef distributed
    !
interface loopback 0
    ip address 142.6.142.2 255.255.255.255
    !
interface ATM2/0/0
    no ip address
    !
interface ATM2/0/0.22 tag-switching
    unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching ip

```

Configuring LSC Hot Redundancy Example

The network topology shown in [Figure 11](#) incorporates two ATM-LSRs in an MPLS network. This topology includes two LSCs on each BPX node and four edge LSRs.

The following configuration examples show the label-switching configuration for both standard downstream-on-demand interfaces and downstream on demand over a VP-tunnel. The difference between these two types of configurations is as follows:

- Standard interface configuration configures a VPI range of one or more VPIs while LDP control information flows in PVC 0,32.

- VP-tunnel configures a single VPI (such as vpi 12) and uses a **tag-switching atm control-vc of vpi,32** global configuration command (for example, 12,32). You can use a VP-tunnel to establish label-switching neighbor relationships through a private ATM cloud.

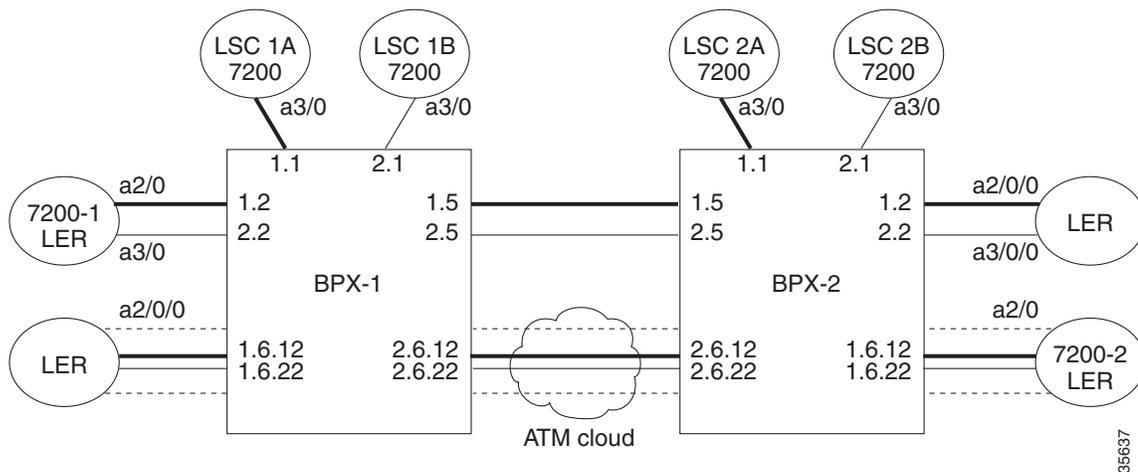
The following configuration examples are provided in this section:

- [LSC 1A Configuration](#)
- [LSC 1B Configuration](#)
- [LSC 2A Configuration](#)
- [LSC 2B Configuration](#)
- [BPX1 and BPX2 Configuration](#)
- [Edge LSR 7200-1 Configuration](#)
- [Edge LSR 7500-1 Configuration](#)
- [Edge LSR 7500-2 Configuration](#)
- [Edge LSR 7200-2 Configuration](#)

For the IGX, use the following commands:

```
extended-port atm1/0 descriptor 0.x.x.0
tag-control-protocol vsi slaves 32 id x
```

Figure 11 ATM-LSR Network Configuration Example



Note

In the following configuration examples for the LSCs, you can use the **tag-switching request-tags for** global configuration command instead of the **tag-switching atm disable-headend-vc** global configuration command.

LSC 1A Configuration

```
7200 LSC 1A:
ip cef
!
tag-switching atm disable-headend vc
!
interface loopback0
ip address 192.103.210.5 255.255.255.255
!
```

```

interface ATM3/0
  no ip address
  tag-control-protocol vsi id 1
!
interface XTagATM12
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 1.2
  tag-switching atm vpi 2-5
  tag-switching ip
!
interface XTagATM15
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 1.5
  tag-switching atm vpi 2-15
  tag-switching ip
!
interface XTagATM1612
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 1.6.12
  tag-switching atm vp-tunnel 12
  tag-switching ip
!
interface XTagATM2612
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.6.12
  tag-switching atm vp-tunnel 12
  tag-switching ip

```

LSC 1B Configuration

```

7200 LSC 1B:
ip cef
!
tag-switching atm disable-headend vc
!
!
interface loopback0
ip address 192.103.210.6 255.255.255.255
!
interface ATM3/0
  no ip address
  tag-control-protocol vsi id 2
!
interface XTagATM22
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.2
  tag-switching atm vpi 2-5
  tag-switching ip
!
interface XTagATM25
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.5
  tag-switching atm vpi 2-15
  tag-switching ip
!
interface XTagATM1622
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 1.6.22
  tag-switching atm vp-tunnel 22
  tag-switching ip
!
interface XTagATM2622
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.6.22

```

```

tag-switching atm vp-tunnel 22
tag-switching ip

```

LSC 2A Configuration

```

7200 LSC 2A:
ip cef
!
tag-switching atm disable-headend vc
!
interface loopback0
ip address 192.103.210.7 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi id 1
!
interface XTagATM12
ip unnumbered loopback0
extended-port ATM3/0 bpx 1.2
tag-switching atm vpi 2-5
tag-switching ip
!
interface XTagATM15
ip unnumbered loopback0
extended-port ATM3/0 bpx 1.5
tag-switching atm vpi 2-15
tag-switching ip
!
interface XTagATM1612
ip unnumbered loopback0
extended-port ATM3/0 bpx 1.6.12
tag-switching atm vp-tunnel 12
tag-switching ip
!
interface XTagATM2612
ip unnumbered loopback0
extended-port ATM3/0 bpx 2.6.12
tag-switching atm vp-tunnel 12
tag-switching ip

```

LSC 2B Configuration

```

7200 LSC 2B:
ip cef
!
tag-switching atm disable-headend vc
!
interface loopback0
ip address 192.103.210.8 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi id 2
!
interface XTagATM22
ip unnumbered loopback0
extended-port ATM3/0 bpx 2.2
tag-switching atm vpi 2-5
tag-switching ip
!
interface XTagATM25
ip unnumbered loopback0
extended-port ATM3/0 bpx 2.5

```

```

tag-switching atm vpi 2-15
tag-switching ip
!
interface XTagATM1622
 ip unnumbered loopback0
 extended-port ATM3/0 bpx 1.6.22
 tag-switching atm vp-tunnel 22
 tag-switching ip
!
interface XTagATM2622
 ip unnumbered loopback0
 extended-port ATM3/0 bpx 2.6.22
 tag-switching atm vp-tunnel 22
 tag-switching ip

```

BPX1 and BPX2 Configuration

BPX1 and BPX2:

```

uptrk 1.1
 addshelf 1.1 vsi 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
 upln 1.2
upport 1.2
 cnfrsrc 1.2 256 252207 y 1 e 512 6144 2 5 26000 100000
 uptrk 1.5
 cnfrsrc 1.5 256 252207 y 1 e 512 6144 2 15 26000 100000
 uptrk 1.6.12
cnftrk 1.6.12 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,
 RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 12
 cnfrsrc 1.6.12 256 252207 y 1 e 512 6144 12 12 26000 100000
 uptrk 1.6.22
cnftrk 1.6.22 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,
 RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 22
 cnfrsrc 1.6.22 256 252207 y 2 e 512 6144 22 22 26000 100000
 uptrk 2.1
 addshelf 2.1 vsi 2 2
cnfrsrc 2.1 256 252207 y 2 e 512 6144 2 15 26000 100000
 upln 2.2
upport 2.2
 cnfrsrc 2.2 256 252207 y 2 e 512 4096 2 5 26000 100000
 uptrk 2.5
 cnfrsrc 2.5 256 252207 y 2 e 512 6144 2 15 26000 100000
 uptrk 2.6.12
cnftrk 2.6.12 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,
 RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 12
 cnfrsrc 2.6.12 256 252207 y 1 e 512 6144 12 12 26000 100000
 uptrk 2.6.22
cnftrk 2.6.22 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,
 RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 22
 cnfrsrc 2.6.22 256 252207 y 2 e 512 6144 22 22 26000 100000

```



Note

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XtagATM port for the VSI partition (for example, XtagATM11).

Edge LSR 7200-1 Configuration

```

7200-1 edge LSR:
 ip cef
 !
 interface loopback0

```

```

ip address 192.103.210.1 255.255.255.255
!
interface ATM2/0
    no ip address
!
interface ATM2/0.12 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching ip
!
interface ATM3/0
    no ip address

interface ATM3/0.22 tag-switching
    ip unnumbered loopback 0
    tag-switching atm vpi 2-5
    tag-switching ip

```

Edge LSR 7500-1 Configuration

```

7500-1 edge LSR:
    ip cef distributed
    !
    interface loopback0
    ip address 192.103.210.2 255.255.255.255
    !
    interface ATM2/0/0
        no ip address
    !
    interface ATM2/0/0.1612 tag-switching
    ip unnumbered loopback0
        tag-switching atm vp-tunnel 12
        tag-switching ip
    !
    interface ATM2/0/0.1622 tag-switching
    ip unnumbered loopback0
        tag-switching atm vp-tunnel 22
        tag-switching ip

```

Edge LSR 7500-2 Configuration

```

7500-2 edge LSR:
    ip cef distributed
    !
    interface loopback0
    ip address 192.103.210.3 255.255.255.255
    !
    interface ATM2/0/0
        no ip address
    !
    interface ATM2/0/0.12 tag-switching
    ip unnumbered loopback0
        tag-switching atm vpi 2-5
        tag-switching ip
    !
    !
    interface ATM3/0/0
        no ip address
    !
    interface ATM3/0/0.22 tag-switching
    ip unnumbered loopback0
        tag-switching atm vpi 2-5
        tag-switching ip

```

Edge LSR 7200-2 Configuration

```

7200-2 edge LSR:
  ip cef
  !
  interface loopback0
  ip address 192.103.210.4 255.255.255.255
  !
  interface ATM2/0
  no ip address
  !
  interface ATM2/0.1612 tag-switching
  ip unnumbered loopback0
  tag-switching atm vp-tunnel 12
  tag-switching ip
  !
  interface ATM2/0.1622 tag-switching
  ip unnumbered loopback0
  tag-switching atm vp-tunnel 22
  tag-switching ip

```

Configuring LSC Warm Standby Redundancy Example

The configuration of LSC Warm Standby redundancy can be implemented by configuring the redundant link for either a higher routing cost than the primary link or configuring a bandwidth allocation that is less desirable. This needs to be performed only at the edge LSR nodes, because the LSCs have been configured to disable the creation of headend VCs, which reduces the LVC overhead.

Configuring an Interface Using Two VSI Partitions Example

A special case may arise where a network topology can only support a neighbor relationship between peers using a single trunk or line interface. To configure the network, perform the following steps:

- Step 1** Configure the interface to use both VSI partitions. The VSI partition configuration for the interface must be made with no overlapping VP space. For example, for interface 2.8 on the ATM-LSR, the following configuration is required:

```

uptrk 2.8
  cnfrsrc 2.8 256 252207 y 1 e 512 6144 2 15 26000 100000
  cnfrsrc 2.8 256 252207 y 2 e 512 6144 16 29 26000 100000

```

Thus partition 1 will create LVCs using VPIs 2-15 and partition 2 will create LVCs using VPIs 16-29.

- Step 2** Configure the control-vc. Each LSC requires a control VC (default 0,32); however, only one LSC can use this default control-vc for any one trunk interface. The following command forces the control VC assignment.

```
tag-switching atm control-vc <vpi>,<vci>
```

Therefore, LSC 1 XTagATM28 can use the default control-vc 0,32 (but it is suggested that you use 2,32 to reduce configuration confusion) and the LSC 2 XTagATM28 should use control-vc 16,32.

For the IGX, use the following commands:

```

extended-port atm1/0 descriptor 0.x.x.0
tag-control-protocol vsi slaves 32 id x

```

The following example shows the configuration steps:

LSC1 Configuration

```
interface XTagATM2801
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.8
  tag-switching atm vpi 2-15
      tag-switching atm control-vc 2 32
tag-switching ip
```

LSC2 Configuration

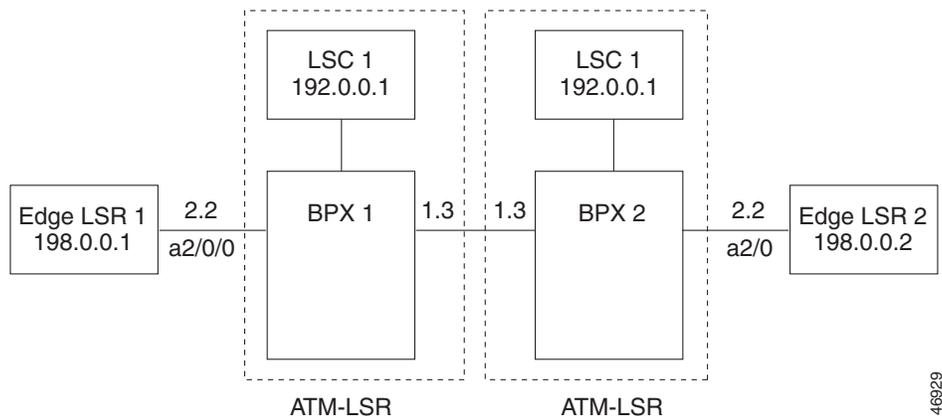
```
interface XTagATM2802
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.8
  tag-switching atm vpi 16-29
      tag-switching atm control-vc 16 32
tag-switching ip
```

Using an Access List to Control the Creation of Headend VCs

The following example shows how to use an access list to control the creation of headend VCs in an MPLS network, which allows the network to support more destinations.

Figure 12 shows two edge LSRs and two ATM-LSRs. In the configuration, only LSPs between edge LSRs are required to provide label switched paths. Other LSPs are not essential. The LSPs between LSCs and between the LSCs and the edge LSRs are often unused and required only for monitoring and maintaining the network. In such cases the IP forwarding path is sufficient.

Figure 12 Sample MPLS Network



In networks that require connections only between edge LSRs, you can use the access list to eliminate the creation of unnecessary LSPs. This allows LVC resources to be conserved so that more edge LSR connections can be supported.

To prevent creation of LSPs between LSCs, create an access list that denies all 192.0.0.0/24 addresses. Then, to prevent creation of LVCs from the LSCs to the edge LSRs, create an access list that denies all 198.0.0.0/24 addresses. The configuration examples for LSC 1 and 2 show the commands for performing these tasks.

To prevent creation of LVCs from the edge LSRs to LSCs, create an access list at the edge LSRs that denies all 192.0.0.0/24 addresses. The configuration examples for edge LSR 1 and 2 show the commands for performing this task.

LSC 1 Configuration

```
7200 LSC1:
  ip cef
  !
  tag-switching request-tags for acl_lsc
  ip access-list standard acl_lsc
  deny 192.0.0.0 0.255.255.255
  deny 198.0.0.0 0.255.255.255
  permit any
  !
  interface loopback0
  ip address 192.0.0.1 255.255.255.255
  !
  interface ATM3/0
  no ip address
  tag-control-protocol vsi
  !
  interface XTagATM13
  extended-port ATM3/0 bpx 1.3
  ip unnumbered loopback0
  tag-switching atm vpi 2-15
  tag-switching ip
  !
  interface XTagATM22
  extended-port ATM3/0 bpx 2.2
  ip unnumbered loopback0
  tag-switching atm vpi 2-5
  tag-switching ip
```

BPX1 and BPX2 Configuration

```
BPX1 and BPX2:
  uptrk 1.1
  addshelf 1.1 v 1 1
  cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
  uptrk 1.3
  cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
  uptrk 2.2
  cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000
```



Note

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XtagATM port for the VSI partition (for example, XtagATM11).

LSC 2 Configuration

```
7200 LSC2:
  ip cef
  !
  tag-switching request-tags for acl_lsc
  ip access-list standard acl_lsc
  deny 192.0.0.0 0.255.255.255
  deny 198.0.0.0 0.255.255.255
  permit any
  !
  interface loopback0
  ip address 192.0.0.2 255.255.255.255
```

```

!
interface ATM3/0
  no ip address
  tag-control-protocol vsi
!
interface XTagATM13
  extended-port ATM3/0 bpx 1.3
  ip unnumbered loopback0
  tag-switching atm vpi 2-15
  tag-switching ip
!
interface XTagATM22
  extended-port ATM3/0 bpx 2.2
  ip unnumbered loopback0
  tag-switching atm vpi 2-5
  tag-switching ip
!

```

Edge LSR 1 Configuration

```

7500 LSR1:
  ip cef distributed
  !
  tag-switching request-tags for acl_ler
  ip access-list standard acl_ler
  deny 192.0.0.0 0.255.255.255
  permit any
  !
  interface loopback 0
  ip address 198.0.0.1 255.255.255.255
  !
  interface ATM2/0/0
  no ip address
  !
  interface ATM2/0/0.22 tag-switching
  ip unnumbered loopback 0
  tag-switching atm vpi 2-5
  tag-switching ip

```

Edge LSR 2 Configuration

```

7200 LSR2:
  ip cef
  !
  tag-switching request-tags for acl_ler
  ip access-list standard acl_ler
  deny 192.0.0.0 0.255.255.255
  permit any
  !
  interface loopback 0
  ip address 198.0.0.2 255.255.255.255
  !
  interface ATM2/0
  no ip address
  !
  interface ATM2/0.22 tag-switching
  ip unnumbered loopback 0
  tag-switching atm vpi 2-5
  tag-switching ip

```

MPLS Egress NetFlow Accounting Example

In the following example, the VPN routing and forwarding (VRF) instances currently configured in the router is displayed:

```
Router# show ip vrf

      Name                               Default RD           Interfaces
-----
vpn1                                100:1                Ethernet1/4
                               Loopback1
vpn3                                300:1                Ethernet1/2
                               Loopback2

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface eth1/4
Router(config-if)# mpls ?
    ip                Configure dynamic MPLS forwarding for IP
    label-protocol    Configure label/tag distribution protocol (LDP/TDP)
    mtu               Set tag switching Maximum Transmission Unit
    netflow           Configure Egress Netflow Accounting
    traffic-eng       Configure Traffic Engineering parameters

Router(config-if)# mpls net
Router(config-if)# mpls netflow ?
    egress            Enable Egress Netflow Accounting
```

MPLS egress NetFlow accounting is enabled on interface eth1/4 and debugging is turned on, as follows:

```
Router(config-if)# mpls netflow egress
Router(config-if)#
Router(config-if)#
Router# debug mpls netflow
MPLS Egress NetFlow debugging is on
Router#
```

The following example shows the current configuration in the router:

```
Router# show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

ip cef
no ip domain-lookup
!
```

The VRF is defined, as follows:

```
ip vrf vpn1
  rd 100:1
  route-target export 100:1
  route-target import 100:1
!
interface Loopback0
  ip address 41.41.41.41 255.255.255.255
  no ip directed-broadcast
  no ip mroute-cache
!
```

```
interface Ethernet1/4
 ip vrf forwarding vpn1
 ip address 180.1.1.1 255.255.255.0
 no ip directed-broadcast
 mpls netflow egress
!
```

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



MPLS Label Switch Controller and Enhancements

This document describes the Cisco Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC). It describes the MPLS LSC feature, identifies the platforms supported by the MPLS LSC, provides configuration examples for MPLS LSC components, and describes related IOS commands that can be used with the supported platforms.

Feature History for MPLS Label Switch Controller and Enhancements

Release	Modification
11.1CT	This document was introduced as the <i>Tag Switch Controller</i> .
12.0(3)T	Added references to the Cisco IOS switching services documentation.
12.0(5)T	Added support for multi-VCs.
12.0(7)DC	Added support for the Cisco 6400 UAC. Added support for virtual trunking/tunneling. Added support for dedicated LSC with the command mpls atm disable-headend-vc .
12.1(3)T	Added support for LSC redundancy.
12.1(5)T	Added access list support for controlling the creation of label switch paths with the command mpls request-labels for . Added support for Cisco IGX 8410, 8420, and 8430 switches. Removed support for the 7500 router as an MPLS LSC.
12.2(4)T	Changed tag-switching commands and terminology to MPLS format. Added support for Cisco MGX 8850 switch with the Cisco MGX RPM-PR card as an MPLS LSC. Added DiffServ with MPLS QoS multi-VC feature support. Added the vc-range keyword to the mpls atm vpi and mpls atm vp-tunnel commands. Extended the VPI range from 256 to 4095.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Release	Modification
12.2(8)T1	Added support for the Cisco 8400 IGX Switch with a Universal Router Module as an MPLS ATM-LSR. Added support for the VC merge and MPLS Diff-Serv-aware features.
12.3(2)T	Added support for the MPLS OAM Insertion and Loop Detection on LC-ATM feature. Modified the oam-pvc and oam retry commands.
12.3(2)T6	Added the LVC Path Trace feature. Added the path keyword to the show mpls atm-ldp bindings command.
12.3(9)	This feature was integrated into 12.3(9).
12.4(20)T	Support was removed for this feature in Cisco IOS Release 12.4(20)T and later releases.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Document Organization

This document is organized as follows. The following sections describe MPLS LSC in general:

- [Feature Overview, page 4](#)
- [Platforms Supported by MPLS LSC, page 8](#)
- [Supported Standards, MIBs, and RFCs, page 9](#)
- [Configuration Tasks, page 9](#)

The following sections describe MPLS LSC features. Each section contains its own configuration steps and examples:

- [Feature 1: Creating Virtual Trunks, page 64](#)
- [Feature 2: Using LSC Redundancy, page 72](#)
- [Feature 3: Reducing the Number of Label Switch Paths Created in an MPLS Network, page 89](#)
- [Feature 4: Differentiated Services and MPLS QoS Multi-VCs, page 95](#)
- [Feature 5: MPLS VC Merge, page 106](#)
- [Feature 6: MPLS Diff-Serv-Aware Traffic Engineering over ATM, page 108](#)
- [Feature 7: MPLS: OAM Insertion and Loop Detection on LC-ATM, page 111](#)
- [Feature 8: Troubleshooting the MPLS LSC Network with the LVC Path Trace Feature, page 115](#)

The following section provides additional information for the Cisco MGX 8850 RPM-PR:

- [Starting Up the Cisco MGX 8850 PXM-45 and Cisco MGX AXSM, page 117](#)

The following sections describe commands used throughout the book:

- [Command Reference, page 126](#)
- [Glossary, page 128](#)

Changing from Tag-Switching to MPLS Terminology

Cisco is moving from tag-switching to MPLS, because MPLS is compliant with the IETF standard. This change necessitates terminology and command changes. [Table 1](#) lists the old tag-switching terms and the equivalent MPLS terms used in this document.

Table 1 *Equivalency Table for Tag-Switching and MPLS Terms*

Old Tag Switching Terminology	New MPLS Terminology
Tag Switching	MPLS, Multiprotocol Label Switching
Tag (short for Tag Switching)	MPLS
TDP (Tag Distribution Protocol)	LDP (Label Distribution Protocol) Cisco TDP and LDP (MPLS Label Distribution Protocol) are nearly identical in function, but use incompatible message formats and some different procedures. Cisco is changing from TDP to a fully compliant LDP.
Tag Switched	Label Switched
TFIB (Tag Forwarding Information Base)	LFIB (Label Forwarding Information Base)
TSR (Tag Switching Router)	LSR (Label Switching Router)
TSC (Tag Switch Controller)	LSC (Label Switch Controller)
ATM-TSR (ATM Tag Switch Router)	ATM-LSR (ATM Label Switch Router, such as the Cisco BPX 8650 switch)
TVC (Tag VC, Tag Virtual Circuit)	LVC (Label VC, Label Virtual Circuit)
TSP (Tag Switch Path)	LSP (Label Switch Path)

Feature Overview

The MPLS label switch controller (LSC), combined with the slave ATM switch, supports scalable integration of IP services over an ATM network. The MPLS LSC enables the slave ATM switch to:

- Participate in an MPLS network
- Directly peer with IP routers
- Support the IP and MPLS features in Cisco IOS software

The MPLS LSC supports highly scalable integration of MPLS (IP+ATM) services by using a direct peer relationship between the ATM switch and MPLS routers. This direct peer relationship removes the limitation on the number of IP edge routers (typical of traditional IP-over-ATM networks), allowing service providers to meet growing demands for IP services. The MPLS LSC also supports direct and rapid implementation of advanced IP and MPLS services over ATM networks using ATM switches.

MPLS combines the performance and virtual circuit capabilities of Layer 2 (data link layer) switching with the scalability of Layer 3 (network layer) routing capabilities. This combination enables service providers to deliver solutions for managing growth, providing differentiated services, and leveraging existing networking infrastructures.

The MPLS LSC architecture provides the flexibility to:

- Run MPLS applications over Layer 2 technologies
- Support any Layer 3 protocol while scaling the network to meet future needs

By deploying the MPLS LSC across large enterprise networks or wide area networks, customers can:

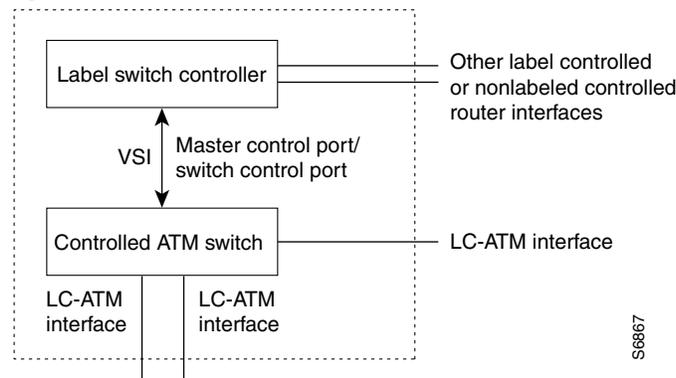
- Save money by using existing ATM infrastructures
- Grow revenue using MPLS-enabled services
- Increase productivity through enhanced network scalability and performance

MPLS LSC Functional Description

The MPLS LSC is a label switch router (LSR) that is configured to control the operation of a separate ATM switch. Together, the MPLS LSC and the controlled ATM switch function as a single ATM label switch router (ATM-LSR).

Figure 1 shows the functional relationship between the MPLS LSC and the ATM switch that it controls.

Figure 1 MPLS Label Switch Controller and Controlled ATM Switch



The following routers can function as an MPLS LSC:

- Cisco 7200 series router
- Cisco 6400 Universal Access Concentrator (UAC)

The following ATM switches can function with the Cisco 7200 series router as the controlled ATM switch:

- Cisco BPX 8600, 8650 (which includes a Cisco 7204 router), and 8680
- Cisco IGX 8410, 8420, and 8430

Also, the Cisco MGX 8850 switch with a Cisco MGX 8850 Route Processor Module (RPM-PR) can function as an MPLS ATM-LSR.

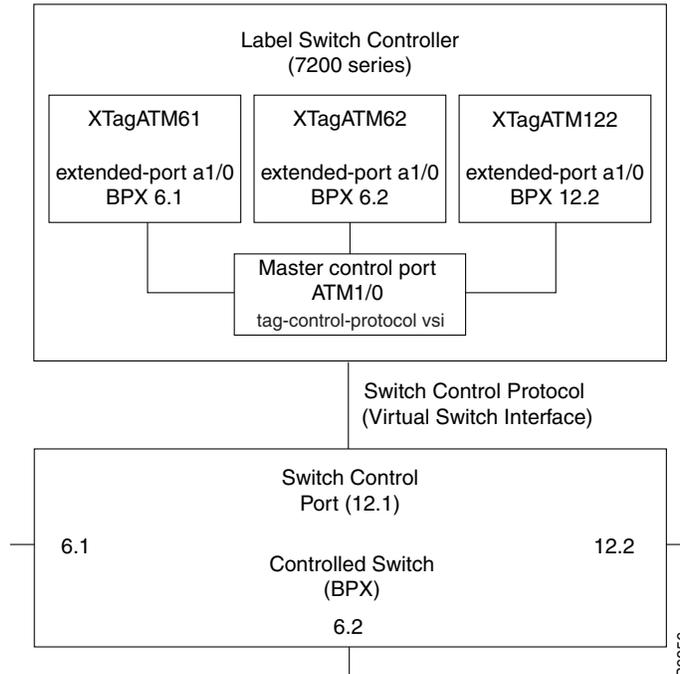
The MPLS LSC controls the ATM switch by means of the Virtual Switch Interface (VSI), which runs over an ATM link connecting the two devices.

The dotted line in Figure 1 represents the logical boundaries of the external interfaces of the MPLS LSC and the controlled ATM switch, as discovered by the IP routing topology. The controlled ATM switch provides one or more XTagATM interfaces at this external boundary. The MPLS LSC can incorporate other label-controlled or nonlabel-controlled router interfaces.

Using Controlled ATM Switch Ports as Router Interfaces

The XTagATM ports on the LSC are used as an IOS interface type called extended Label ATM (XTagATM). To associate these XTagATM interfaces with particular physical interfaces on the controlled ATM switch, use the interface configuration command **extended-port**.

Figure 2 shows a typical MPLS LSC configuration that controls three ATM ports on a Cisco BPX switch: ports 6.1, 6.2, and 12.2. These corresponding XTagATM interfaces were created on the MPLS LSC and associated with the corresponding ATM ports on the Cisco BPX switch by means of the **extended-port** command.

Figure 2 Typical MPLS LSC and BPX Switch Configuration

Observe from [Figure 2](#) that:

- An additional port on the Cisco BPX switch (port 12.1) acts as the switch control port.
- An ATM interface (ATM1/0) on the MPLS LSC acts as the master control port.

How the LSC, ATM Switch, and VSI Work Together

The LSC and slave ATM switch have the following characteristics:

- The LSC runs all of the control protocols.
- The ATM switch forwards the data.
- Each physical interface on the slave ATM switch maps to an XTagATM interface on the LSC. Each XTagATM interface is configured to have a dedicated LDP session with a corresponding interface on an edge or core device. The XTagATM interfaces are mapped in the routing topology, and the ATM switch behaves as a router.
- The LSC can also function as an Edge LSR. The data for the Edge LSR passes through the control interface of the router.

If a component on the LSC fails, the ATM switch's IP switching function is disabled. The standalone LSC is the single point of failure.

The VSI implementation includes the following characteristics:

- The VSI allows multiple, independent control planes to control a switch. The VSI ensures that the control processes (SS7, MPLS, PNNI, and so on) can act independently of each other by using a VSI slave process to control the resources of the switch and apportion them to the correct control planes.
- In MPLS, each physical interface on the slave ATM switch maps to an XTagATM interface on the LSC through the VSI. In other words, physical interfaces are mapped to their respective logical interfaces.

- The routing protocol on the LSC generates route tables entries. The master sends connection requests and connection release requests to the slave based on routing table entries.
- The slave sends the configured bandwidth parameters for the ATM switch interface to the master in the VSI messages. The master includes the bandwidth information in the link state topology. You can override these bandwidth values by manually configuring the bandwidth on the XTagATM interfaces on the LSC.

MPLS LSC Benefits

Using the MPLS LSC provides the following benefits:

- **IP-ATM Integration**—Enables ATM switches to directly support advanced IP and MPLS services and protocols, thereby reducing operational costs and bandwidth requirements, while at the same time decreasing time-to-market for new services.
- **Virtual Private Networks (VPNs)**—Supports IP-based VPNs on an integrated IP+ATM backbone or a gigabit router backbone.
- The following services over an ATM MPLS network:
 - Any Transport over MPLS (AToM) services
 - Diff-Serve traffic engineering services
 - LLSP-based Diff-Serve multi-vc MPLS services
 - Layer 3 MPLS VPN services

MPLS LSC Restrictions

- **Supporting ATM Forum Protocols**—You can connect the MPLS LSC to a network that is running ATM Forum protocols while the MPLS LSC simultaneously performs its functions. However, you must connect the ATM Forum network through a separate ATM interface (that is, not through the master control port).
- **Cannot Use the MPLS LSC as an Edge Router**—Using the MPLS LSC as a label edge device is *not* supported. Using the MPLS LSC as a label edge device introduces unnecessary complexity to the network design, configuration, and performance. See [“Disabling the LSC from Acting as an Edge LSR” section on page 63](#) to disable edge LSR functionality on the LSC.
- **Using Static Routes in the ATM MPLS network:** When you create static routes in the ATM MPLS network, if the forwarding router is a LSC, it must be a next-hop router to the ingress router. If the forwarding router is an ATM edge router, it can be located anywhere in the network. When creating static routes with the following command, the forwarding router’s address can be a PE router’s address.

```
ip route destination-prefix destination-mask forwarding-router's-address
```



Note

Configuring static routes on the LSC is not supported.

- **Enable CEF on the control ATM interface:** When you configure the control ATM interface for an XtagATM interface, enable CEF switching on that interface. Issue the **ip route cache** command `cef` to enable CEF.

Related Documents

The following documents provide more information about MPLS features:

- [MPLS QoS Multi-VC Mode for PA-A3](#)
- [MPLS Label Distribution Protocol](#)
- [Using OAM for PVC Management](#)
- [Troubleshooting PVC Failures When Using OAM Cells and PVC Management](#)

The following documents provide more information about platform-specific features:

Cisco 6400 UAC

- [Configuring Multiprotocol Label Switching on the Cisco 6400 UAC](#)

Cisco BPX 8600 Series Switches

- [Cisco MPLS Controller Software Configuration Guide, Version 9.3.0 and 9.3.10](#)

Cisco IGX 8400 Series Switches

- [Update to the Cisco IGX 8400 Series Installation and Configuration Guide and Cisco IGX 8400 Series Reference Guide, Version 9.3.0](#)
- [Update to the Cisco IGX 8400 Series Reference Guide, Version 9.3.0](#)

Cisco MGX 8850 Route Processor Module

- [Cisco MGX Route Processor Module Installation and Configuration Guide, Version 2.1](#)

Cisco IGX 8400 Series Switches with a URM

- [Cisco IGX 8400 Series Installation Guide](#)
- [Cisco IGX 8400 Series Provisioning Guide](#)

Platforms Supported by MPLS LSC

Routers

You can use the following routers to configure an ATM-LSR:

- Cisco 7200 series routers—Support the following interface:
 - ATM Port Adapter (PA-A1 and PA-A3)
- Cisco 6400 Universal Access Concentrator—Supports the following interfaces:
 - DS-3
 - OC-3/STM-1
 - OC-12/STM-4
- Cisco MGX 8850 RPM-PR as an LSC

Switches

You can use the following ATM switches to configure an ATM-LSR:

- Cisco BPX 8600, 8650, and 8680 switches

- Cisco IGX 8410, 8420, and 8430 switches with the Cisco 7200 series routers

Switches with Router Modules

You can also use the following switches with router modules as ATM-LSRs:

- Cisco MGX 8850 switch with the Cisco 8850 Route Processor Module (RPM-PR)
- Cisco IGX 8410, 8420, and 8430 switches with a Universal Router Module (URM)

Supported Routing Protocols on LC-ATM and MPLS LSC

The following protocols are supported on the LC-ATM and MPLS LSC:

- OSPF
- ISIS

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://www.cisco.com/go/mibs>

RFCs:

- RFC 3031, Multiprotocol Label Switching Architecture
- RFC 3036, LDP Specification
- RFC 3035, MPLS using LDP and ATM VC Switching

Configuration Tasks

See the following for examples of basic configuration tasks for enabling MPLS LSC functionality:

- [Configuring the 7200 Series LSCs for BPX and IGX Switches](#)
- [Configuring the Cisco MGX 8850 Switch and RPM-PR as an MPLS LSC](#)
- [Configuring the Cisco 6400 Universal Access Concentrator as an MPLS LSC](#)
- [Configuring the Cisco IGX 8400 Switch with a Universal Router Module as an MPLS ATM-LSR](#)
- [Disabling the LSC from Acting as an Edge LSR](#)

Refer to the Cisco BPX 8600 or IGX 8400 series switch documentation for BPX/IGX switch configuration examples.

Configuring the 7200 Series LSCs for BPX and IGX Switches

To enable MPLS functionality on the Cisco 7200 series routers connected to BPX and IGX switches, perform the following steps on each LSC in the configuration.


Note

If you are configuring for LSC redundancy, ensure that the controller ID matches the slave and is unique to the LSC system. Also, make sure that the VPI/VCI value for the control VC matches its peer

	Command	Purpose
Step 1	<pre>Router(config)# interface loopback0 Router(config-if)# ip address 172.103.210.5 255.255.255.255 Router(config-if)# exit</pre>	<p>Creates a software-only loopback interface that emulates an interface that is always up. Specify an interface number for the loopback interface. There is no limit on the number of loopback interfaces you can create.</p> <p>Assigns an IP address to Loopback0. It is important that all loopback addresses in an MPLS network are host addresses, that is, with a mask of 255.255.255.255. Using a shorter mask can prevent MPLS-based VPN services from working correctly.</p>
Step 2	<pre>Router(config)# mpls atm disable-headend-vc</pre>	<p>Prevents the router from assigning headend VCs for each destination prefix. With downstream on demand, MPLS ATM networks LVCs are a limited resource that are easily depleted with the addition of each new node.</p>
Step 3	<pre>Router(config)# interface atm1/0 Router(config-if)# tag-control-pro TOCOL vsi id 1</pre>	<p>Creates an ATM interface (atm1/0).</p> <p>Configures a Virtual Switch Interface (VSI) on (atm1/0). The VSI ID is 1. The VSI ID must match the controller ID you assign to the ATM switch.</p> <p>For the IGX switch, use tag-control-protocol vsi slaves 32 id 1</p>
Step 4	<pre>Router(config-if)# interface XTagATM61 Router(config-if)# ip route-cache cef Router(config-if)# extended-port atm1/0 bpx 6.1</pre>	<p>Creates an XTagATM interface (XTagATM61.)</p> <p>Enables CEF on the XTagATM interface.</p> <p>Associates the XTagATM interface with an external interface (BPX port 6.1) on the remotely controlled ATM switch atm1/0 identifies the ATM interface used to control the remote ATM switch.</p> <p>For the IGX switch, use the extended-port atm1/0 descriptor 0.6.1.0 or extended-port atm1/0 igx command.</p>
Step 5	<pre>Router(config-if)# ip unnumbered loopback0</pre>	<p>Makes XTagATM61 an unnumbered interface and use the IP address of loopback 0 as a substitute. The interfaces in an ATM MPLS network should usually be unnumbered. This reduces the number of IP destination-prefixes in the routing table, which reduces the number of labels and LVCs used in the network.</p>

	Command	Purpose
Step 6	<pre>Router(config-if)# mpls ip Router(config-if)# mpls atm vpi 2-5 Router(config-if)# exit</pre>	<p>Enables MPLS on the XTagATM interface.</p> <p>Limits the range of VPIs so that the total does not exceed 4 between an Edge LSR and an LSC. For example: mpls atm vpi 2-5 mpls atm vpi 10-13</p> <p>The VPI range total can be 12 or 13 between LSCs. The range depends on how many VCs the interface can support.</p>
Step 7	<pre>Router(config-if)# interface XTagATM1222 Router(config-if)# extended-port atm1/0 bpx 12.2.2</pre>	<p>Configures MPLS on another XTagATM virtual interface and binds it to BPX virtual trunk interface 12.2.2.</p> <p>For the Cisco IGX switch, use extended-port atm1/0 descriptor 0.12.2.2 or extended-port atm1/0 igx.</p>
Step 8	<pre>Router(config-if)# ip unnumbered loopback0</pre>	<p>Makes XTagATM1222 an unnumbered interface and use the IP address of loopback 0 as a substitute. The interfaces in an ATM MPLS network should usually be unnumbered. This reduces the number of IP destination-prefixes in the routing table, which reduces the number of labels and LVCs used in the network.</p>
Step 9	<pre>Router(config-if)# mpls atm vp-tunnel 2 Router(config-if)# mpls ip Router(config-if)# exit</pre>	<p>Enables MPLS on the XTagATM interface using a VP-tunnel interface.</p> <p>This will limit the VPI to only vpi = 2. The command will also map the label ATM control VC to 2,32.</p>
Step 10	<pre>Router(config)# ip cef</pre>	<p>Enables Cisco Express Forwarding (CEF).</p>
Step 11	<pre>Router(config)# ip routing Router(config)# router OSPF 100</pre>	<p>Enables IP routing.</p> <p>Enables the OSPF routing protocol. Alternatively, you can enable the IS-IS routing protocol (router isis).</p>

Verifying the MPLS LSC Configuration

The following sections explain some of the commands you can use to ensure that you have configured MPLS correctly.

Check that the Switch Control Port Is Active

Enter the **show controllers vsi status** command to show the switch control port is active. If an interface has been discovered by the LSC, but an XTagATM interface has not been associated with it through the **extended-port** configuration command, then the interface name is marked <unknown>, and interface status is marked n/a.

The following is sample output from the **show controllers vsi status** command:

```
Router# show controllers vsi status
Interface Name          IF Status   IFC State   Physical Descriptor
switch control port    n/a        ACTIVE      12.1.0
XTagATM0                up         ACTIVE      12.2.0
XTagATM1                up         ACTIVE      12.3.0
<unknown>              n/a        FAILED-EXT  12.4.0
```

Check that VSI Sessions Are Established

Make sure that every VSI session has been established. A session consists of an exchange of VSI messages between the VSI master (the LSC) and a VSI slave (an entity on the switch). There can be multiple VSI slaves for a switch. On the ATM switch, each port or trunk card assumes the role of a VSI slave.

The following is sample output from the **show controllers vsi session** command. Session State indicates the status of the session between the master and the slave.

- ESTABLISHED is the fully operational steady state.
- UNKNOWN indicates that the slave is not responding.

Router# **show controllers vsi session**

Interface	Session	VCD	VPI/VCI	Switch/Slave Ids	Session State
ATM0/0	0	1	0/40	0/1	ESTABLISHED
ATM0/0	1	2	0/41	0/2	ESTABLISHED
ATM0/0	2	3	0/42	0/3	DISCOVERY
ATM0/0	3	4	0/43	0/4	RESYNC-STARTING
ATM0/0	4	5	0/44	0/5	RESYNC-STOPPING
ATM0/0	5	6	0/45	0/6	RESYNC-UNDERWAY
ATM0/0	6	7	0/46	0/7	UNKNOWN
ATM0/0	7	8	0/47	0/8	UNKNOWN
ATM0/0	8	9	0/48	0/9	CLOSING
ATM0/0	9	10	0/49	0/10	ESTABLISHED
ATM0/0	10	11	0/50	0/11	ESTABLISHED
ATM0/0	11	12	0/51	0/12	ESTABLISHED

Check that the VSI Is Operational

To display information about the switch interface discovered by the MPLS LSC through VSI, use the **show controllers vsi descriptor EXEC** command. The field called IFC state shows the operational state of the interface, according to the switch. It should be ACTIVE.

Router# **show controllers vsi descriptor 12.2.0**

```
Phys desc: 12.2.0
Log intf: 0x000C0200 (0.12.2.0)
Interface: XTagATM0
IF status: up                IFC state: ACTIVE
Min VPI: 1                   Maximum cell rate: 10000
Max VPI: 259                 Available channels: 2000
Min VCI: 32                  Available cell rate (forward): 10000
Max VCI: 65535               Available cell rate (backward): 10000
```

Check XTagATM Interfaces

Ensure that the control VC 0/32 has been created to carry non-IP traffic (LDP) on every XTagATM interface. The columns marked VCD, VPI, and VCI display information for the corresponding private VC on the control interface. The private VC connects the XTagATM VC to the external switch. It is termed private because its VPI and VCI are only used for communication between the MPLS LSC and the switch, and it is different from the VPI and VCI seen on the XTagATM interface and the corresponding switch port.

Router# **show XTagatm vc**

AAL / Control Interface

Interface	VCD	VPI	VCI	Type	Encapsulation	VCD	VPI	VCI	Status
XTagATM0	1	0	32	PVC	AAL5-SNAP	2	0	33	ACTIVE
XTagATM0	2	1	33	TVC	AAL5-MUX	4	0	37	ACTIVE

```
XTagATM0          3      1      34  TVC  AAL5-MUX          6      0      39  ACTIVE
```

To gather more information about the XTagATM interface, enter the **show interface XTagATM** command:

```
Router# show interface XTagATM0
```

```
XTagATM0 is up, line protocol is up
  Hardware is TAG-Controlled Switch Port
  Interface is unnumbered. Using address of Loopback0 (10.0.0.17)
  MTU 4470 bytes, BW 156250 Kbit, DLY 80 usec, rely 255/255, load 1/255
  Encapsulation ATM Labelswitching, loopback not set
  Encapsulation(s): AAL5
  Control interface: ATM1/0, switch port: bpx 10.2
  9 terminating VCs, 16 switch cross-connects
  Switch port traffic:
    129302 cells input, 127559 cells output
  Last input 00:00:04, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Terminating traffic:
    5 minute input rate 1000 bits/sec, 1 packets/sec
    5 minute output rate 0 bits/sec, 1 packets/sec
    61643 packets input, 4571695 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    53799 packets output, 4079127 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffers copied, 0 interrupts, 0 failures
```

Check that LDP Is Operational

The **show mpls ldp discovery** privileged EXEC command displays the interfaces over which the LDP discovery process is running. Each interface should display a status of “xmit/recv”, which means the LSC is sending and receiving LDP messages.

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
  8.1.1.1:0
Discovery Sources:
  Interfaces:
    Ethernet1/1/3 (ldp): xmit/recv
      LDP Id: 172.73.0.77:0
      LDP Id: 172.16.0.44:0
      LDP Id: 172.22.0.55:0
    ATM3/0.1 (ldp): xmit/recv
      LDP Id: 192.168.7.7:2
    ATM0/0.2 (tdp): xmit/recv
      TDP Id: 192.168.0.1:1
Targeted Hellos:
  10.1.1.1 -> 172.44.0.33 (ldp): active, xmit/recv
      LDP Id: 172.44.0.33:0
  10.1.1.1 -> 192.168.0.16 (tdp): passive, xmit/recv
      TDP Id: 192.168.0.33:0
```

To display the status of LDP sessions, issue the **show mpls ldp neighbor** privileged EXEC command. The output should show that the LDP sessions are operational and sending and receiving messages.

```
Router# show mpls ldp neighbor
```

```

Peer LDP Ident: 192.1680.7.7:2; Local LDP Ident 8.1.1.1:1
  TCP connection: 192.168.7.7.11032 - 8.1.1.1.646
  State: Oper; Msgs sent/rcvd: 5855/6371; Downstream on demand
  Up time: 13:15:09
  LDP discovery sources:
    ATM3/0.1
Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.1:0
  TCP connection: 10.1.1.1.646 - 10.1.1.1.11006
  State: Oper; Msgs sent/rcvd: 4/411; Downstream
  Up time: 00:00:52
  LDP discovery sources:
    Ethernet1/0/0
  Addresses bound to peer LDP Ident:
    10.0.0.29      10.1.1.1      109.0.0.199    172.102.1.1
    10.205.0.9

```

Check that MPLS and LDP Are Operational

Make sure that MPLS is globally enabled and that a label distribution protocol is running on the requested interfaces by issuing the **show mpls interfaces** command.

```

Router# show mpls interfaces
Interface          IP              Tunnel  Operational
(...)
Serial0/1.1        Yes (ldp)       Yes     Yes
Serial0/1.2        Yes             Yes     No
Serial0/1.3        Yes (ldp)       Yes     Yes
(...)

```

The IP field shows that MPLS IP is configured for an interface. The Label Distribution Protocol (LDP) appears in parentheses to the right of the IP status.

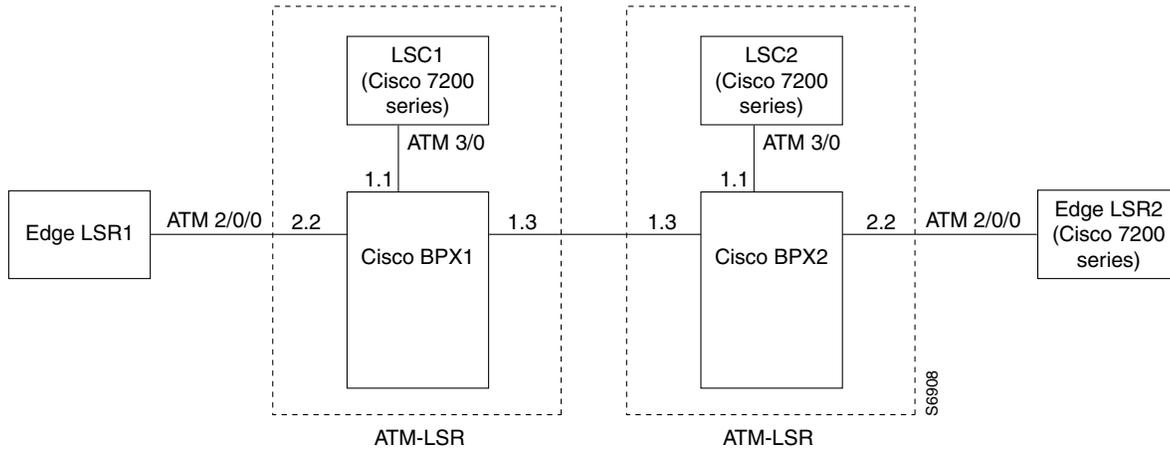
The Tunnel field indicates the capacity of traffic engineering on the interface.

The Operational field shows the status of the LDP. The interface Serial0/1.2 is down in the example; therefore, the Operational field shows that LDP is not operational on that interface.

Configuration Example: MPLS LSC

The network topology shown in [Figure 3](#) incorporates two ATM-LSRs in an MPLS network. This topology includes two LSCs (Cisco 7200 routers), two BPX switches, and two Edge LSRs (Cisco 7200 routers).

Figure 3 ATM-LSR Network Configuration Example



Configuration for LSC1

7200 LSC1:

```

ip cef
!
mpls atm disable-headend vc
!
interface loopback0
 ip address 172.103.210.5 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
 extended-port ATM3/0 bpx 1.3
 ip unnumbered loopback0
 mpls atm vpi 2-15
 mpls ip
!
interface XTagATM22
 extended-port ATM3/0 bpx 2.2
 ip unnumbered loopback0
 mpls atm vpi 2-5
 mpls ip

```

Configuration for BPX1 and BPX2

BPX1 and BPX2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3
cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```

**Note**

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for instance, XTagATM11).

Configuration for LSC2

7200 LSC2:

```
ip cef
!
mpls atm disable-headend vc
!
interface loopback0
    ip address 172.18.143.22 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
    extended-port ATM3/0 bpx 1.3
    ip unnumbered loopback0
    mpls atm vpi 2-15
    mpls ip
!
interface XTagATM22
    extended-port ATM3/0 bpx 2.2
    ip unnumbered loopback0
    mpls atm vpi 2-5
    mpls ip
```

Configuration for Edge LSR1

LSR1:

```
ip cef distributed
!
interface loopback 0
    ip address 172.22.132.2 255.255.255.255
!
interface ATM2/0/0
    no ip address
!
interface ATM2/0/0.5 mpls
    ip unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip
```

Configuration for Edge LSR2

7200 LSR2:

```
ip cef
interface loopback 0
    ip address 172.22.172.18 255.255.255.255
!
interface ATM2/0
    no ip address
!
```

```
interface ATM2/0.9 mpls
  ip unnumbered loopback 0
  mpls atm vpi 2-5
  mpls ip
```

Configuring the Cisco MGX 8850 Switch and RPM-PR as an MPLS LSC

You can configure the Cisco MGX 8850 switch with the Cisco 8850 Router Processor Module (RPM-PR) as an MPLS LSC in an MPLS network.

The RPM-PR provides integrated IP in an ATM platform, enabling services such as integrated Point-to-Point Protocol (PPP), Frame Relay termination, and IP virtual private networks (VPNs) using MPLS technology. It provides Cisco IOS-based multiprotocol routing over ATM, Frame Relay and ATM Interface Layer 3 Termination, Local Server Interconnect over High-Speed LANs, access concentration, and switching between Ethernet LANs and the WAN facilities of the MGX 8850. The RPM-PR runs Cisco IOS software.

The hardware that supports MPLS LSC functionality on the Cisco MGX 8850 switch is described in the following sections.

Cisco MGX 8850 RPM-PR Overview

The RPM-PR is a router module based on an NPE-400 processor, modified to fit into any full-height module slot on a Cisco MGX 8850 32-slot chassis. It connects to the PXM-45 back card, the 4E/B back card, and other service modules through the midplane. The RPM-PR receives power from the midplane and communicates over the midplane with the PXM-45 using IPC over ATM.

The RPM-PR has an integrated ATM interface—a permanently attached ATM port adapter/back card based on the Cisco ATM Deluxe module—and the RPM-PR can support up to two optional back cards to provide LAN connectivity.

The MGX 8850 shelf can be completely populated with 12 RPM-PRs. This allows you to use multiple RPM-PRs to achieve load sharing. Load sharing is achieved by manually distributing connections across multiple embedded RPM-PR router blades.



Note

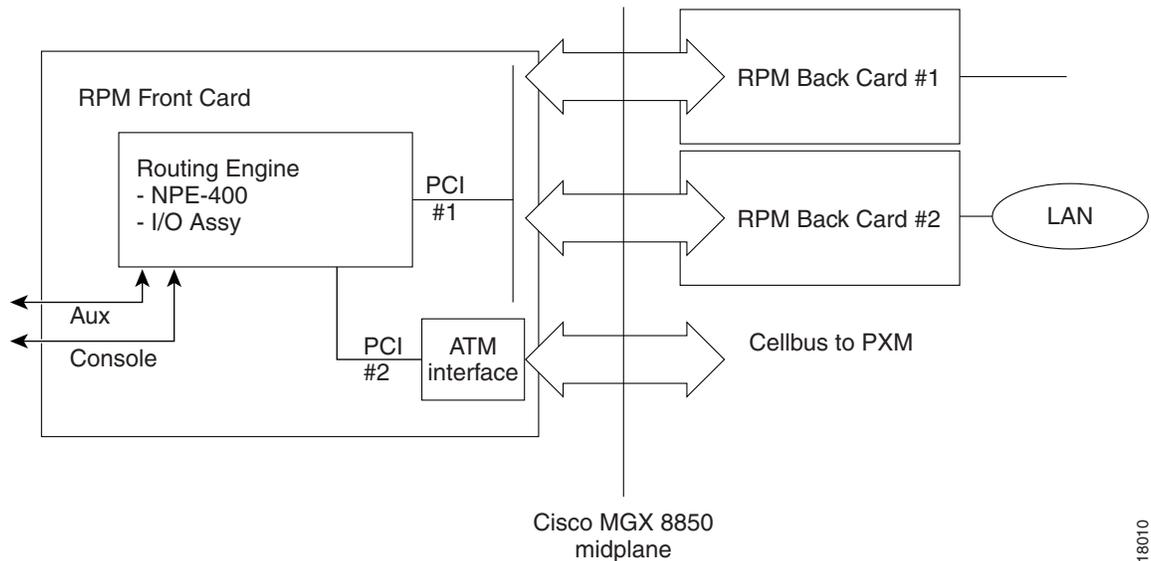
In a 32-slot MGX 8850 configuration, slots 7 and 8 are reserved for the PXM-45 cards occupying the full height of the chassis. Slots 15, 16, 31, and 32 are reserved for Service Redundancy Modules (SRMs).

In a 16-slot configuration, you can add RPM-PRs in any of slots 1 through 6 and 9 through 14. RPM-PRs must not be added to slots 7, 8, 15, or 16 in the MGX 8850 switch.

The RPM-PR fits into the Cisco MGX 8850 and MGX 8850 midplane architecture so that the front card provides Cisco IOS router services, and the back cards provide physical network connectivity. The RPM-PR front card also provides ATM connectivity to the Cisco MGX 8850 cellbus at full-duplex OC-3.

[Figure 4](#) shows a Cisco MGX 8850 RPM-PR connected to the Cisco MGX 8850 midplane and the back cards.

Figure 4 PRM-PR Connected to the MGX 8850 Midplane and to Back Cards



The RPM-PR back cards are connected to the front card by a dual PCI bus (see [Figure 4](#)). Each RPM-PR card can be equipped with up to two single-height back cards.



Note

Slots 7 and 8 are reserved for the PXM-45/B cards occupying the full height of the chassis. You can use PXM-45-UI-S3 cards in the top slots and T3 cards in the bottom slots. You can use MGX-RJ45-FE cards in the top slots and MGX-RJ45-4E/B cards in the bottom slots.



Note

The RPM-PR card within the MGX 8850 chassis supports online insertion and removal of the MGX-RJ45-4E/B and the FE back cards. However, the ATM port adapter is inside the RPM-PR.

MGX 8850 Cellbus

The MGX 8850 cellbus in the MGX 8850 midplane communicates between the RPM-PR, service modules (cellbus slaves) and the PXM-45 (cellbus master) (see [Figure 4](#)). Each cellbus is connected to a set of PXM-45 cards. Only one cellbus can be active at a time.

Communication from master to slaves consists of a broadcast to all slaves. The first byte of the cell header contains addressing information. Each slave will monitor data traffic and “pick up” cells that are destined to its slot. Also, a multicast bit allows all slaves to receive a cell simultaneously.

Communication from the slaves to the master is more complicated. Because many slaves might attempt to transmit simultaneously, arbitration among slaves is required. At the start of a given cell period, the master will poll all slaves to see if they have anything to send. By the end of the current cell, the master will grant, or allow, one of the slaves to transmit. Polling and data transmission occur simultaneously.

If two RPM-PRs in adjacent slots share the same cellbus, you need to configure a clock rate of 42 MHz on the PXM-45.

Use the **dspcbclk** command to display the clock rate:

```
PXM> dspcbclk
```

CellBus	Rate (MHz)	Slots	Allowable Rates (MHz)
CB1	21	1, 2	21, 42
CB2	21	3, 4	21, 42
CB3	21	5, 6	21, 42
CB4	21	17 - 22	21
CB5	21	9, 10	21, 42
CB6	21	11, 12	21, 42
CB7	21	13, 14	21, 42
CB8	21	25 - 30	21

Use the **cnfcbclk cbn 42** command to change the clock rate, where *n* is the number of the cellbus:

```
PXM> cnfcbclk cb1 42
```

CellBus	Rate (MHz)	Slots	Allowable Rates (MHz)
CB1	42	1, 2	21, 42
CB2	21	3, 4	21, 42
CB3	21	5, 6	21, 42
CB4	21	17 - 22	21
CB5	21	9, 10	21, 42
CB6	21	11, 12	21, 42
CB7	21	13, 14	21, 42
CB8	21	25 - 30	21

ATM Deluxe Integrated Port Adapter

The ATM deluxe port adapter provides a single ATM interface to the MGX 8850 cellbus interface (CBI). The ATM port adapter is a permanent, internal ATM interface. As such, it has no cabling to install and does not support interface types. It connects internally and directly to the MGX 8850 midplane.

Comparing Cisco 7200 LSC Configuration with Cisco RPM-PR LSC Configuration

This section compares the configuration of the Cisco 7200 LSC controlling Cisco BPX or Cisco IGX switches with the configuration of the Cisco MGX 8850 RPM-PR LSC controlling the Cisco MGX 8850 switch.

[Table 2](#) compares the configuration of switch partitions and partition resources for the Cisco 7200 LSC controlling the Cisco BPX or Cisco IGX switch with the configuration of the Cisco MGX 8850 RPM-PR LSC controlling the Cisco MGX 8850 switch.

Table 2 *Configuring Partitions and Partition Resources*

Platform	Configuration
Cisco 7200 routers as LSC for Cisco BPX and Cisco IGX switches	<p>Configure VSI MPLS partitioning and resources at the Cisco BPX or Cisco IGX switch, respectively. No switch partition or switch resource is configured at the Cisco 7200 LSC.</p> <p>The following example adds the LSC controller in slot 1 port 1 of the Cisco BPX switch:</p> <pre>uptrk 1.1 addshelf 1.1 v 1 1 cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000</pre> <p>The following example configures slot 2 port 2 of the Cisco BXM for XtagInt in the LSC:</p> <pre>uptrk 2.2 cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000</pre>
Cisco MGX 8850 RPM-PR as LSC in Cisco MGX 8850 switch	<p>In contrast, configure the following at the RPM-PR (router):</p> <ul style="list-style-type: none"> • Partitions—MPLS and Private Network-Network Interface (PNNI) • Partition resources—Interface bandwidth and interface resources, virtual path identifier (VPI), and virtual channel identifier (VCI) <p>The following commands configure the LSC controller ID (8), the switch partition ID (2), and the partition resources in the PRM-PR:</p> <pre>interface Switch1 tag-control-protocol vsi id 8 ip route-cache cef switch partition vcc 2 8 ingress-percentage-bandwidth 1 100 egress-percentage-bandwidth 1 100 vpi 0 0 vci 32 3808</pre> <p>Add the LSC controller in the PXM-45 card using the addcontroller <i><cntrlrtid></i> <i><i o></i> <i><cntrlrType></i> <i><slot></i> <i><cntrlrName></i> command, for example:</p> <pre>SWITCH.7.PXM45.a>addcontroller 8 i 3 5 LSC1</pre>

**Note**

In the Cisco MGX 8850 switch, you configure the partition resources of the switch ports in the RPM-PR. In the Cisco BPX or Cisco IGX switch, you configure all the resources in the switch.

Table 3 compares the configuration of interfaces and virtual paths and identifiers of the Cisco 7200 LSC controlling the Cisco BPX or Cisco IGX switch with the configuration of the Cisco MGX 8850 RPM-PR LSC controlling the Cisco MGX 8850 switch.

Table 3 *Configuring Interfaces and Virtual Path Identifiers/Ranges*

Platform	Configuration
Cisco 7200 routers as LSC for Cisco BPX and Cisco IGX switches	<p>Configure the Xtag interfaces the same as you would for an Edge LSR. No difference exists in the LSC configuration for the User-Network Interface (UNI), the Network-to-Network Interface (NNI), or the virtual template (VT) interfaces.</p> <p>Use any VPI or VPI range or virtual path (VP) tunnel.</p>
Cisco MGX 8850 RPM-PR as LSC in Cisco MGX 8850 switch	<p>With the Cisco 8850 RPM-PR connected directly to the PXM-45 (in the same Cisco MGX 8850 switch), use VPI = 0 for MPLS with virtual channel connection (VCC) partitioning. For this connection, use VPI = 0, VCI = 32 to 3808 for all Xtag interfaces. In the LSC, you cannot use any other VPI or VP tunnel between directly connected RPM-PRs and PXM-45s.</p> <p>With Cisco MGX 8850 AXSM ports used with the Xtag interfaces, configure all UNI, NNI and Virtual Network-Network Interface (VNNI) connections in the same way that you configure them for Cisco BPX and IGX switches. You can configure any VPI, VPI range, and VP tunnel. In addition, you can configure virtual path connections (VPCs), or virtual channel connections (VCCs), or both.</p> <p>Use a descriptor (instead of the bpx or igx in a Cisco BPX or IGX command) when you configure an extended port command for an Xtag interface for the Cisco MGX 8850 switch. Use the following command if the PXM and RPM-PR are in the same Cisco MGX 8850 switch:</p> <pre>Router(config)# extended-port Switch1 descriptor "9.1"</pre> <p>Use this command if the Xtag interface is controlling the AXSM card in a different Cisco MGX 8850 switch:</p> <pre>Router(config)# extended-port Switch1 descriptor "1:1.1:1"</pre> <p>In both cases, you may need to enter the show controller vsi descriptor command to get the correct port number.</p>

Comparing Edge Label Switch Router Configurations

This section compares the configuration of the Cisco 7200 routers, and the Cisco 12000 Internet routers as an Edge Label Switch Router (Edge LSR) with the configuration of the Cisco MGX8850 RPM-PR as an Edge LSR.

Table 4 compares the Edge LSR configuration of the Cisco 7200 routers, and the Cisco 12000 Internet routers with the Cisco MGX 8850 RPM-PR when connected to another RPM-PR and when connected to other routers, such as the Cisco 7200 router.

Table 4 *Edge Label Switch Router Configuration Comparisons*

Platform	Configuration
Cisco 7200, and Cisco 12000 routers	<p>Provision the permanent virtual circuits (PVCs) and permanent virtual paths (PVPs) manually. Once you create a PVC or PVP you can run MPLS on the PVC or PVP. With MPLS, you can configure the following:</p> <ul style="list-style-type: none"> • On the PVCs—Packet MPLS Downstream Unsolicited Tag Distribution Protocol (TDP) or Label Distribution Protocol (LDP) • On the PVPs—Label-controlled ATM (LC-ATM) interface Downstream on Demand TDP or LDP
Cisco MGX 8850 RPM-PR	<p>Create signaled connections, soft permanent virtual circuit (SPVC) and soft permanent virtual path (SPVP) connections, using PNNI between Cisco MGX 8850 RPM-PRs. For this type of connection with VPC partitions, use any VPI = 1 to 256. You can run MPLS on SPVCs or SPVPs. With MPLS, you can configure the following:</p> <ul style="list-style-type: none"> • On the SPVCs—Packet MPLS Downstream Unsolicited TDP or LDP • On the SPVPs—LC-ATM Downstream on Demand TDP or LDP
Connecting Cisco MGX RPM-PR Edge LSR to other routers	<p>Connect the Cisco RPM-PR Edge LSR with other routers (such as the Cisco 7200 router, the Cisco 12000 router, or the Cisco BPX or Cisco IGX switch with the Cisco 7200 router) through AXSM or AXSM-E cards. These routers cannot use PNNI signaling. Therefore, you need to do the following:</p> <ul style="list-style-type: none"> • Start the SPVCs and SPVPs from the RPM-PR and terminate them in the AXSM or AXSM-E cards. (PNNI signaling makes the connection between the RPM-PR and the AXSM or AXSM-E cards.) • Provision the PVC and PVP connections manually at the Cisco 7200, and Cisco 12000 routers, and the Cisco BPX or Cisco IGX switch with the Cisco 7200 router.

Configuring the Cisco MGX RPM-PR

This section provides the following configuration information for the Cisco MGX RPM-PR:

- [Accessing the RPM-PR Command Line Interface, page 22](#)
- [Booting the RPM-PR, page 23](#)
- [RPM-PR Bootflash Precautions, page 23](#)
- [Configuring the Cisco MGX 8850 Switch with RPM-PR to Perform Basic LSC Operations, page 24](#)

Accessing the RPM-PR Command Line Interface

To configure the RPM-PR, you must access the command line interface (CLI) of the RPM-PR.

You can access the RPM-PR CLI using any of the following methods:

- Console port on the front of the RPM-PR.
- `cc` from another MGX 8850 card.
- Telnet from a workstation, PC, or another router.

Booting the RPM-PR

When the RPM-PR is booted, the boot image must be the first file in the bootflash. (See the section “[RPM-PR Bootflash Precautions](#)” to make sure that the first file on the bootflash is a valid boot image.) If the bootflash does not have a valid boot image as a first file, the card may not be able to boot and can result in bootflash corruption. If the bootflash is corrupted, you need to send the card back for an external burn with a valid boot image.

You can reboot the RPM-PR from the PXM by entering the **resetcd** *<card_number>* command from the switch CLI, where *card_number* is the slot number of the RPM-PR that is being rebooted.



Caution

Omitting the card number resets the entire system.

Also, you can reboot the RPM-PR from the RPM-PR using the RPM-PR console port and entering the **reload** command.



Note

The **boot system bootflash**:*<filename>* command loads the run-time software from the bootflash. The **boot system E**:*<filename>* command loads the run-time software from the PXM-45 hard disk. You can use either command to load the run-time software.

In addition, you can use the regular TFTP boot procedures to boot the RPM-PR. Make sure you have the network connection to the tftpboot server first.

RPM-PR Bootflash Precautions

The RPM-PR bootflash is used to store boot image, and possibly configuration and run-time files. The bootflash stores and accesses data sequentially, and the RPM-PR boot image must be the first file stored to successfully boot the card.

The RPM's boot image, which comes loaded on the bootflash, will work for all RPM IOS images, and therefore, no reason exists to delete or move the factory-installed boot image.



Caution

Erasing or moving the boot image can cause RPM-PRs to fail to boot. When this happens, the RPM must be returned to Cisco and reflashed.

To avoid unnecessary failures, requiring card servicing, you should:

- Never erase the boot file from the RPM bootflash.
- Never change the position of the boot file on the RPM bootflash.
- Use care when “squeezing” the bootflash to clean it up.

As long as the boot file remains intact in the first position on the bootflash, the RPM will successfully boot.



Note

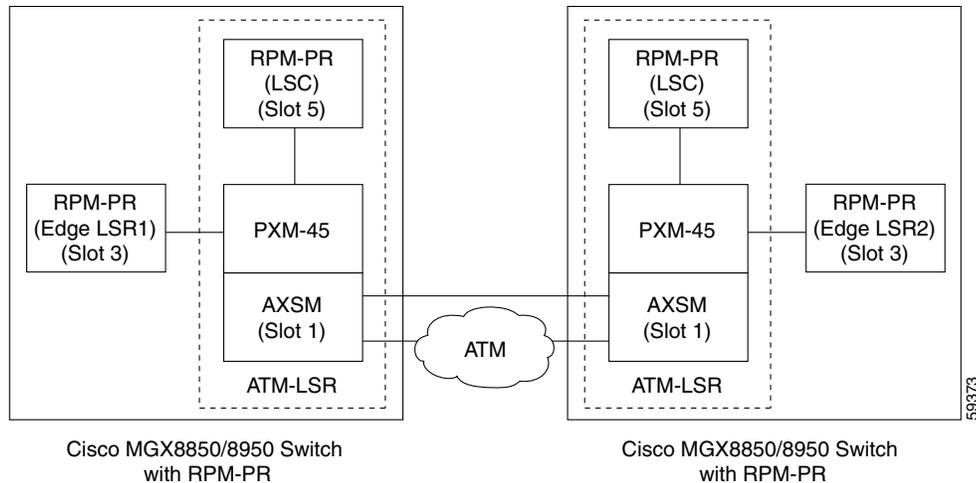
The **boot system bootflash**:*<filename>* command loads the run-time software from the bootflash. The **boot system E**:*<filename>* command loads the run-time software from the PXM-45 hard disk. You can use either command to load the run-time software.

Configuring the Cisco MGX 8850 Switch with RPM-PR to Perform Basic LSC Operations

To support MPLS on the Cisco 8850 switch, you need to configure MPLS support on the RPM-PR, the PXM-45, and the AXSM cards.

Figure 5 shows a Cisco MGX 8850 switch with a Cisco MGX 8850 RPM-PR set up to perform basic MPLS LSC functions. The following sections contain configuration steps and examples that show the setup of MPLS support on the Cisco MGX 8850 switch with a Cisco MGX RPM-PR.

Figure 5 Typical Cisco MGX 8850 Configuration to Support MPLS LSC Functions



Note

If two RPM-PRs in adjacent slots share the same cellbus, you need to configure a clock rate of 42 MHz on the PXM-45. Use the `dspcbclk` command to display the clock rate. Use the `cnfcbclk cbn 42` command to change the clock rate, where *n* is the number of the cellbus.

Configuration Steps: Adding an MPLS Controller to the PXM-45

To add an MPLS controller to the PXM-45 card, follow these steps:

	Command	Purpose
Step 1	MGX8850.7.PXM.a> addcontroller 8 i 3 5 LSC1	Identifies a network control protocol to the VSI that runs on the node. This control protocol is identified by an ID of 8 (possible, 3 to 20), as an internal (i) MPLS controller (3), located in slot 5. The name of the controller is LSC1.
Step 2	MGX8850.7.PXM.a> cc 5 Router> enable Password: Router# config terminal	Switches to the router (RPM-PR card). Accesses the configuration mode of the router. Enter configuration commands, one per line. End with Ctrl/Z.
Step 3	Router(config)# ip cef	Enables Cisco Express Forwarding (CEF).

	Command	Purpose
Step 4	Router(config)# interface loopback0 Router(config-if)# ip address 28.28.28.28 255.255.255.255	Creates a software-only loopback interface that emulates an interface that is always up. Specify an interface number for the loopback interface. There is no limit on the number of loopback interfaces you can create. Assigns an IP address to Loopback0. It is important that all loopback addresses in an MPLS network are host addresses, that is, with a mask of 255.255.255.255.
Step 5	Router(config-if)# interface switch1 Router(config-if)# no ip address Router(config-if)# tag-control-protocol vsi id 8 Router(config-if)# ip route-cache cef	Creates an ATM interface (switch1) without an IP address. Configures a VSI on switch1. The VSI ID is 8. The VSI ID must match the controller ID you assign to the ATM switch. Enables CEF on that interface.
Step 6	Router(config-if)# switch partition vcc 2 8	Configures the resource partition for the controller with a partition ID of 2. The controller ID (8) is the ID set with the addcontroller command.
Step 7	Router(config-if-swpart)# ingress-percentage-bandwidth 1 100 Router(config-if-swpart)# egress-percentage-bandwidth 1 100	Sets the ingress bandwidth percentage and the egress bandwidth percentage 1 to 100 percent for the controller.
Step 8	Router(config-if-swpart)# vpi 0 0 Router(config-if-swpart)# vci 32 3808	Sets the VPI/VCI ranges for the controller.
Step 9	Router(config-if-swpart)# Ctrl1/Z	Exits configuration mode.

When you use the Cisco MGX 8850 RPM-PR as an MPLS LSC, you also need to add and partition an AXSM NNI port for MPLS.

Configuration Example: Adding and Partitioning an AXSM NNI Port for MPLS

The following example shows adding and then partitioning an NNI port on an AXSM card for MPLS.

```
cc 1
cnfcdsct 4
upln 1.1
addport 1 1.1 353207 353207 4 2
addpart 1 2 8 500000 500000 500000 500000 0 15 32 65535 4000 4000
dsparts
```

Where:

- Options for the **cnfcdsct** are 4 = policing on and 5 = policing off for ATM Forum (ATMF) service types.
- The **addport** command syntax is as follows:

```
addport ifNum bay.line guaranteedRate maxRate sctID ifType [vpiNum]
```

where:

ifNum = a number between 1 and 60
bay.line = the Line number
guaranteedRate = the virtual rate in cells/sec
MaxRate = OC48 rate—between 50 and 5651320
 (*maxRate* for OC12 is between 50 and 1412830
maxRate for OC3 is between 50 and 353207
maxRate for T3 is between 50 and 96000 (PLCP), 104268 (ADM)
maxRate for E3 is between 50 and 80000)
sctID = the Port SCT ID between 0 and 255, for default file use 0
ifType = 1 for uni; 2 for nni; 3 for vnni
 (optional) *vpiNum* = between a number 1 and 4095, used for configuring the interface as a virtual trunk

The *guaranteedRate* argument must equal the *maxRate* argument.

- The **addpart** syntax is as follows:

addpart *ifNum partID cntlrID egrminbw egrmaxbw ingrminbw ingrmaxbw minVpi maxVpi minVci maxVci minConns maxConns*

Where:

ifNum = a number between 1 and 60
partID = the Partition Identifier between 1 and 20
cntlrID = the Controller Identifier between 1 and 20
egrminbw = the Egress guaranteed percentage of bandwidth in units of 0.0001% of interface bandwidth
egrmaxbw = the Egress maximum percentage of bandwidth in units of 0.0001% of interface bandwidth
ingrminbw = the Ingress guaranteed percentage of bandwidth in units of 0.0001% of interface bandwidth
ingrmaxbw = the Ingress maximum percentage of bandwidth in units of 0.0001% of interface bandwidth
minVpi = the minimum VPI value, which is a number between 0 and 4095 (0 to 255 for UNI interface)
maxVpi = the maximum VPI value, which is number between 0 and 4095 (0 to 255 for UNI interface)
minVci = the minimum VCI value, which is a number between 32 and 65535
maxVci = the maximum VCI value, which is a number between 32 and 65535
minConns = the guaranteed number of connections, which is a number between 0 and the maximum number of connections in portgroup
maxConns = the maximum number of connections, which is a number between 0 and the maximum number of connections in portgroup

- The **dspparts** command shows the newly added partition and verifies its settings.

Configuration Steps: Mapping an AXSM Port to an XtagATM Interface on the LSC

Enter the following commands into the RPM-PR to map AXSM ports to the LSC:

	Command	Purpose
Step 1	MGX8850.7.PXM.a> cc 5	Switches to the router (RPM-PR card in slot 5).
Step 2	Router> enable Password:	Accesses the router commands.
Step 3	Router# config terminal Router(config)#	Enters the global configuration mode.
Step 4	Router(config)# interface XtagATM1111	Creates an XtagATM interface (XtagATM1111).

	Command	Purpose
Step 5	Router(config-if)# ip unnumbered Loopback0	Makes XtagATM1111 an unnumbered interface and uses the IP address of loopback 0 as a substitute. The interfaces in an ATM MPLS network should usually be unnumbered. This reduces the number of IP destination-prefixes in the routing table, which reduces the number of labels and LVCs used in the network.
Step 6	Router(config-if)# extended-port Switch1 descriptor "1:1.1:1"	Associates the XtagATM interface with an external interface (AXSM port 1.1) on the remotely controlled ATM switch. Switch1 identifies the ATM interface used to control the remote ATM switch. The <i>descriptor</i> format is x:y.z. <ul style="list-style-type: none"> • x = slot where the AXSM is located (1) • y.y = line number (1.1) • z = port number (1) (this is a logical port)
Step 7	Router(config-if)# mpls ip	Enables label switching on AXSM port 1.1.
Step 8	Router(config-if)# Ctrl/Z	Exits configuration mode.

When you use the Cisco MGX 8850 RPM-PR as an MPLS LSC, you also need to create the VNNI port on the AXSM card and add an XtagATM interface on the LSC for the VNNI port.

Configuration Example: Creating the VNNI Port on the AXSM Card

The following example shows the creation of a VNNI port on the AXSM card residing on the PXM-45 shelf.

```
cc 1
cnfcdsct 4
upln 1.2
addport 12 1.2 353207 353207 4 2 11
addpart 12 2 8 250000 250000 250000 250000 11 11 32 65535 10000 10000
dspart 2
```

Where:

- The **addport** command syntax is as follows:

addport *ifNum bay.line guaranteedRate maxRate sctID ifType [vpiNum]*

Where:

```
ifNum = a number between 1 and 60
bay.line = the Line number
guaranteedRate = the virtual rate in cells/sec
MaxRate = OC48 rate—between 50 and 5651320
(maxRate for OC12 is between 50 and 1412830
maxRate for OC3 is between 50 and 353207
maxRate for T3 is between 50 and 96000 (PLCP), 104268 (ADM)
maxRate for E3 is between 50 and 80000)
sctID = the Port SCT ID between 0 and 255, for default file use 0
ifType = 1 for uni; 2 for nni; 3 for vnni
(optional) vpiNum = VPI between 1 and 4095, used for configuring the interface as
a virtual trunk
```

The *guaranteedRate* argument must equal the *maxRate* argument.

- The **addpart** syntax is as follows:

addpart *ifNum partID cntlrID egrminbw egrmaxbw ingrminbw ingrmaxbw minVpi maxVpi minVci maxVci minConns maxConns*

Where:

ifNum = a number between 1 and 60
partID = the Partition Identifier between 1 and 20
cntlrID = the Controller Identifier between 1 and 20
egrminbw = the Egress guaranteed percentage of bandwidth in units of 0.0001% of interface bandwidth
egrmaxbw = the Egress maximum percentage of bandwidth in units of 0.0001% of interface bandwidth
ingrminbw = the Ingress guaranteed percentage of bandwidth in units of 0.0001% of interface bandwidth
ingrmaxbw = the Ingress maximum percentage of bandwidth in units of 0.0001% of interface bandwidth
minVpi = the minimum VPI value, which is a number between 0 and 4095 (0 to 255 for UNI interface)
maxVpi = the maximum VPI value, which is number between 0 and 4095 (0 to 255 for UNI interface)
minVci = the minimum VCI value, which is a number between 32 and 65535
maxVci = the maximum VCI value, which is a number between 32 and 65535
minConns = the guaranteed number of connections, which is a number between 0 and the maximum number of connections in portgroup
maxConns = the maximum number of connections, which is a number between 0 and the maximum number of connections in portgroup

- The **dspart** command shows the newly added partition (2) and verifies its settings.

Configuration Example: Adding an XtagATM Interface on the LSC for the VNNI Port

The following example shows the addition of an XtagATM interface on the Label Switch Controller (LSC) for the VNNI port.

```
cc 5
enable
Password:
config terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
interface XtagATM11212
    ip unnumbered Loopback0
    extended-port Switch1 descriptor "1:1.2:12"
mpls ip
```

Configuration Steps: Configuring an RPM as an Edge Label Switch Router

To configure the RPM-PR as an Edge Label Switch Router (Edge LSR) on the MGX 8850 Release 2 shelf, follow these steps:

	Command	Purpose
Step 1	MGX8850.7.PXM.a> cc 3 Router> enable Password: Router# config terminal	Connects to the router (RPM-PR card). Accesses router commands. Enters the global configuration mode of the router. Enter configuration commands, one per line. End with Ctrl/Z.
Step 2	Router(config)# ip cef	Enables Cisco Express Forwarding (CEF).
Step 3	Router(config)# interface Loopback0 Router(config-if)# ip address 192.168.2.11 255.255.255.255	Creates a software-only loopback interface that emulates an interface that is always up. Specifies an interface number for the loopback interface. There is no limit on the number of loopback interfaces you can create. Assigns an IP address to Loopback0. It is important that all loopback addresses in an MPLS network are host addresses, that is, with a mask of 255.255.255.255.
Step 4	Router(config-if)# switch partition vcc 2 8	Configures the resource partition for the controller with a partition ID of 2. The controller ID (8) is the ID set with the addcontroller command.
Step 5	Router(config-if-swpart)# ingress-percentage-bandwidth 1 100 Router(config-if-swpart)# egress-percentage-bandwidth 1 100	Sets the ingress bandwidth percentage and the egress bandwidth percentage 1 to 100 percent for the controller. This command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.
Step 6	Router(config-if-swpart)# vpi 0 0 Router(config-if-swpart)# vci 32 3808	Sets the VPI/VCI ranges for the controller.
Step 7	Router(config-if-swpart)# Ctrl/Z	Exits partition configuration mode.
Step 8	Router(config)# interface Switch1.11 mpls	Creates a subinterface on the RPM-PR and identifies the type of link. The switch interface number is always 1. The subinterface number (11) must be unique for the RPM-PR. You choose the subinterface number when you create the subinterface.
Step 9	Router(config-if)# ip unnumbered Loopback0	Makes the subinterface an unnumbered interface and uses the IP address of loopback 0 as a substitute.
Step 10	Router(config-if)# mpls ip	Enables MPLS forwarding of IPv4 packets.
Step 11	Router(config-if)# Ctrl/Z	Exits configuration mode.

Configuring an XTag Interface in the LSC Connecting to the RPM-PR Edge LSR

To configure an XTag interface on the LSC connecting to the Cisco MGX 8850 RPM-PR Edge LSR, follow these steps:

	Command	Purpose
Step 1	MGX8850.7.PXM.a> cc 3 Router> enable Password: Router# config terminal	Connects to the router (RPM-PR card). Accesses router commands. Enters the global configuration mode of the router. Enter configuration commands, one per line. End with Ctrl/Z.
Step 2	Router(config)# ip cef	Enables Cisco Express Forwarding (CEF).
Step 3	Router(config)# interface loopback0 Router(config-if)# ip address 10.9.9.9 255.255.255.255	Creates a software-only loopback interface that emulates an interface that is always up. Specifies an interface number for the loopback interface. There is no limit on the number of loopback interfaces you can create. Assigns an IP address to Loopback0. It is important that all loopback addresses in an MPLS network are host addresses, that is, with a mask of 255.255.255.255.
Step 4	Router(config)# interface switch1	Configures an ATM interface (Switch1).
Step 5	Router(config-if)# switch partition vcc 2 8	Configures the resource partition for the controller with a partition ID of 2. The controller ID (8) is the ID set with the addcontroller command.
Step 6	Router(config-if-swpart)# ingress-percentage-bandwidth 1 100 Router(config-if-swpart)# egress-percentage-bandwidth 1 100	Sets the ingress bandwidth percentage and the egress bandwidth percentage 1 to 100 percent for the controller. This command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.
Step 7	Router(config-if-swpart)# vpi 0 0 Router(config-if-swpart)# vci 32 3808	Sets the VPI/VCI ranges for the controller.
Step 8	Router(config-if-swpart)# Ctrl/Z	Exits partition configuration mode.
Step 9	Router(config)# interface XTagATM31	Creates an XTag ATM interface (XTagATM31).
Step 10	Router(config-if)# ip unnumbered Loopback0	Makes the subinterface an unnumbered interface and uses the IP address of loopback 0 as a substitute.
Step 11	Router(config-if)# extended-port switch1 descriptor "3.1"	Associates the XtagATM interface with port 3.1.
Step 12	Router(config-if)# mpls ip	Enables MPLS forwarding of IPv4 packets.
Step 13	Router(config-if)# Ctrl/Z	Exits configuration mode.

MGX ATM MPLS Configuration Examples

This section contains the following sample Cisco MGX 8850 ATM MPLS configurations:

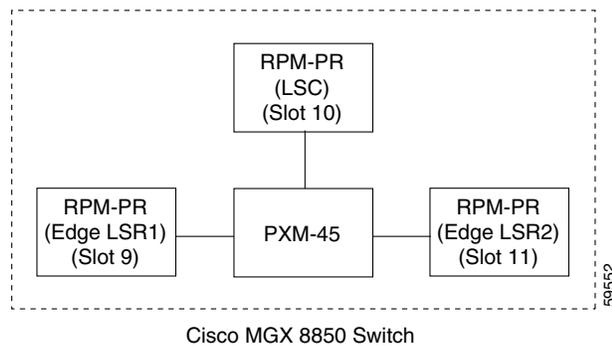
- [Simple Cisco MGX 8850 RPM-PR LSC Network Configuration \(VCC Switch Partition\), page 31](#)
- [Cisco MGX 8850 RPM-PR LSC Network Configuration with Cisco MGX 8850 and Cisco BPX Switches \(VCC Switch Partition\), page 33](#)

Simple Cisco MGX 8850 RPM-PR LSC Network Configuration (VCC Switch Partition)

Figure 6 represents the sample RPM-PR LSC network configuration for a VCC switch partition for the configuration examples that follow.

- [RPM-PR Edge LSR1 Configuration, page 31](#)
- [PXM LSC Configuration, page 32](#)
- [RPM-PR LSC Configuration, page 32](#)
- [RPM-PR Edge LSR2 Configuration, page 33](#)

Figure 6 Sample RPM-PR LSC Network Configuration



Note

If two RPM-PRs in adjacent slots share the same cellbus, you need to configure a clock rate of 42 MHz on the PXM-45. Use the **dspeclk** command to display the clock rate. Use the **cnfcbclk cbn 42** command to change the clock rate, where **n** is the number of the cellbus.

RPM-PR Edge LSR1 Configuration

Following is an example of an RPM-PR Edge LSR(1) configuration. This example uses the **switch partition vcc** command and therefore, only VCI ranges can be used; you cannot use VPI ranges or VP tunnels. In this example, only one label (tag) switching interface is used, so you can use the default VPI = 0 and the VCI range = 32 to 3808.



Note

In the Cisco BPX and IGX switches, you normally use VPI range or VP tunnels or both. In the Cisco MGX 8850 switch, a VCI range is commonly used. In the Cisco MGX 8850 switch, the partition resources of the switch ports are configured at the RPM-PR. In the Cisco BPX or IGX switches, all resources are configured in the switch.

```
ip cef
!
interface Loopback0
 ip address 10.9.9.9 255.255.255.255
!
 interface Switch1
  switch partition vcc 2 8
  ingress-percentage-bandwidth 1 100
  egress-percentage-bandwidth 1 100
  vpi 0 0
  vci 32 3808
!
interface Switch1.1 mpls
```

```

        ip unnumbered Loopback0
        mpls atm vpi 0 vci 33 3000
        mpls ip
    !
router ospf 100
    network 10.0.0.0 0.255.255.255 area 0

```

Where:

- The **switch partition vcc 2 8** command configures a partition ID = 2 and a controller ID = 8.
- The **ingress-percentage-bandwidth 1 100** command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.

PXM LSC Configuration

The following command adds the LSC controller in the PXM-45. Use the **addcontroller <cntrlrtid> <i | o> <cntrlrType> <slot> [cntrlrName]** command:

```
addcontroller 8 i 3 10 LSC
```

Where:

- The controller ID = 8.
- The controller is internal (i).
- The controller type =MPLS (3).
- The slot number = 10.
- The name of the controller = LSC.

RPM-PR LSC Configuration

Following is an example of an RPM-PR LSC configuration. This example uses the **switch partition vcc** command and therefore, you can use only VPI = 0 and VCI ranges; you cannot use VPI ranges or VP tunnels.

```

ip cef
!
mpls atm disable-headend-vc
!
interface Loopback0
    ip address 10.20.20.20 255.255.255.255
!
interface Switch1
tag-control-protocol vsi id 8
ip route-cache cef
switch partition vcc 2 8
ingress-percentage-bandwidth 1 100
egress-percentage-bandwidth 1 100
vpi 0 0
vci 32 3808
!
interface XTagATM91
    ip unnumbered Loopback0
    extended-port Switch1 descriptor 9.1
    mpls ip
!
interface XTagATM111
    ip unnumbered Loopback0
    extended-port Switch1 descriptor 11.1
    mpls ip
!
router ospf 100

```

```
network 10.0.0.0 0.255.255.255 area 0
```

Where:

- The **tag-control-protocol vsi id 8** command configures an LSC controller with an ID = 8.
- The **switch partition vcc 2 8** command configures the VCC partition with an MPLS partition ID = 2. (The LSC controller ID is 8.)
- The **ingress-percentage-bandwidth 1 100** partition resource command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.
- You need to enter a **show controller vsi descriptor** command to get the port number, for example, 9.1, for the **extended-port Switch1 descriptor 9.1** command. If this Xtag interface is controlling the AXSM card, then the format is different. Again, refer to the output from the **show controller vsi descriptor** command.

RPM-PR Edge LSR2 Configuration

Following is an example of an RPM-PR Edge LSR(2) configuration. This example uses the **switch partition vcc** command and therefore, only VPI = 0 and any VCI in the allowed range can be used; you cannot use VPI ranges or VP tunnels.

```
ip cef
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface Switch1
 switch partition vcc 2 8
 ingress-percentage-bandwidth 1 100
 egress-percentage-bandwidth 1 100
 vpi 0 0
 vci 32 3808
!
interface Switch1.1 mpls
 ip unnumbered Loopback0
 mpls atm vpi 0 vci 33 3000
 mpls ip
!
router ospf 100
 network 10.0.0.0 0.255.255.255 area 0
```

Where:

- The **switch partition vcc 2 8** command configures the VCC partition with an MPLS partition ID = 2 and a LSC controller ID = 8.
- The **ingress-percentage-bandwidth 1 100** partition resource command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.

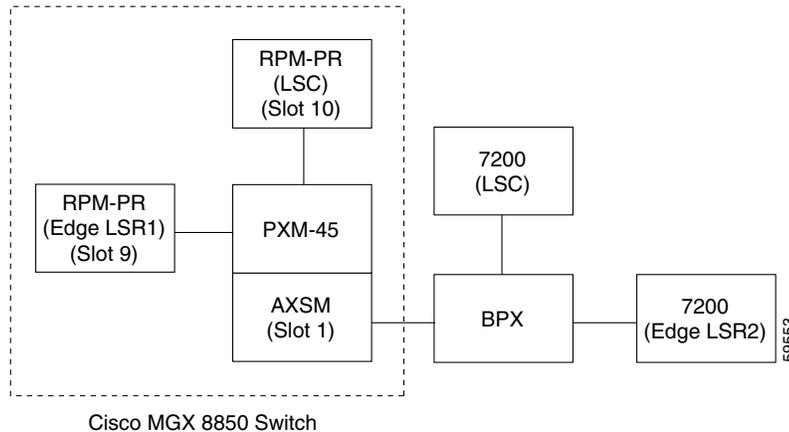
Cisco MGX 8850 RPM-PR LSC Network Configuration with Cisco MGX 8850 and Cisco BPX Switches (VCC Switch Partition)

Figure 7 represents a sample RPM-PR LSC network configuration with the MGX 8850 and the BPX switches for the configuration examples that follow.

- [RPM-PR Edge LSR1 Configuration, page 34](#)
- [PXM LSC Configuration, page 35](#)
- [RPM-PR LSC Configuration, page 35](#)
- [Mapping a Cisco MGX 8850 AXSM Port to an XtagATM Interface on the Cisco MGX 8850 RPM-PR LSC, page 36](#)

- [AXSM Configuration for the Xtag Interfaces, page 36](#)
- [Configuration for BXP, page 37](#)
- [Configuration for Cisco 7200 LSC, page 38](#)
- [Configuration for Cisco 7200 Edge LSR2, page 38](#)

Figure 7 Sample RPM-PR LSC Network with Cisco MGX 8850 and Cisco BPX Switches



Note

If two RPM-PRs in adjacent slots share the same cellbus, you need to configure a clock rate of 42 MHz on the PXM-45. Use the **dspeblk** command to display the clock rate. Use the **cnfcbclk cbn 42** command to change the clock rate, where **n** is the number of the cellbus.

RPM-PR Edge LSR1 Configuration

Following is an example of a PRM-PR Edge LSR(1) configuration. This example uses the **switch partition vcc** command and therefore, you can use only VCI ranges; you cannot use VPI ranges or VP tunnels. In this example, only one label (tag) switching interface is used, so you use the default VPI = 0 and the VCI range = 33 to 3808.



Note

In the Cisco BPX and IGX switches, you normally use a VPI range or VP tunnels or both. In the Cisco MGX 8850 switch, a VCI range is commonly used.

In the Cisco MGX 8850 switch, the partition resources of the switch ports are configured at the RPM-PR. In the Cisco BPX or IGX switches, all resources are configured in the switch.

```

ip cef
!
interface Loopback0
 ip address 10.9.9.9 255.255.255.255
!
interface Switch1
 switch partition vcc 2 8
 ingress-percentage-bandwidth 1 100
 egress-percentage-bandwidth 1 100
 vpi 0 0
 vci 32 3808
!
interface Switch1.1 mpls
  
```

```

    ip unnumbered Loopback0
    mpls atm vpi 0 vci 33 3000
    mpls ip
!
router ospf 100
    network 10.0.0.0 0.255.255.255 area 0

```

Where:

- The **switch partition vcc 2 8** command configures a partition ID = 2 and a controller ID = 8.
- The **ingress-percentage-bandwidth 1 100** partition resource command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.

PXM LSC Configuration

The following command adds the LSC controller in the PXM-45. Use the **addcontroller <ctrlrId> <i | o> <ctrlrType> <slot> [ctrlrName]** command:

```
addcontroller 8 i 3 10 LSC
```

Where:

- The controller has an ID = 8.
- The controller is internal (i).
- The controller type = MPLS (3).
- The slot number = 10.
- The name of the controller = LSC.

RPM-PR LSC Configuration

Following is an example of an RPM-PR LSC configuration. This example uses the **switch partition vcc** command and therefore, you can use only VPI = 0 and VCI ranges: you cannot use VPI ranges or VP tunnels.

```

ip cef
!
mpls atm disable-headend vc
!
interface Loopback0
    ip address 10.20.20.20 255.255.255.255
!
interface Switch1
tag-control-protocol vsi id 8
ip route-cache cef
switch partition vcc 2 8
controller ID is 8.
ingress-percentage-bandwidth 1 100
egress-percentage-bandwidth 1 100
vpi 0 0
vci 32 3808
!
interface XTagATM91
    ip unnumbered Loopback0
    extended-port Switch1 descriptor 9.1
    mpls ip
!
router ospf 100
    network 10.0.0.0 0.255.255.255 area 0

```

Where:

- The **tag-control-protocol vsi id 8** command configures an LSC controller with an ID = 8.
- The **switch partition vcc 2 8** command configures the VCC partition with an MPLS partition ID = 2. (The LSC controller ID is 8.)
- The **ingress-percentage-bandwidth 1 100** partition resource command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.
- You need to enter a **show controller vsi descriptor** command to get the port number, for example, 9.1, for the **extended-port Switch1 descriptor 9.1** command. If this Xtag interface is controlling the AXSM card, then the format is different. Again, refer to the output from the **show controller vsi descriptor** command.

Mapping a Cisco MGX 8850 AXSM Port to an XtagATM Interface on the Cisco MGX 8850 RPM-PR LSC

The following example shows a sample configuration for mapping an AXSM port to an XtagATM interface on the RPM-PR LSC:

```
interface XTagATM1111
    ip unnumbered Loopback0
    extended-port Switch1 descriptor 1:1.1:1
    mpls atm vpi 0-15
    mpls ip
!
router ospf 100
    network 10.0.0.0 0.255.255.255 area 0
```

Where:

- In the **extended-port Switch1 descriptor 1:1.1:1** command, the **descriptor** format is *x:y.z*, where
 - *x* = slot for the AXSM card
 - *y.y* = the line number
 - *z* = the port number (this is a logical port)
- The **mpls atm vpi 0-15** command configures a VPI range of 0 to 15 in the AXSM interface.

AXSM Configuration for the Xtag Interfaces

This configuration example shows adding and partitioning an NNI port on an AXSM card for MPLS. Enter the **cc** command to change to an AXSM card, then enter the **cnfcdsct** command to configure the AXSM card service class template (SCT) for PNNI and MPLS:

At the PXM-45 SWITCH.7PXM.a> prompt:

```
cc 1
```

At the AXM SWITCH.1.AXSM.a> prompt:

```
cnfcdsct 4
upln 1.1
addport 1 1.1 353207 353207 4 2
addpart 1 2 5 500000 500000 500000 500000 0 15 32 65535 4000 4000
dsparts

if part Ctlr egr egr ingr ingr min max min max min max
Num ID ID GuarBw MaxBw GuarBw MaxBw vpi vpi vci vci conn conn
    (.0001%) (.0001%) (.0001%) (.0001%)
-----
1 2 5 500000 500000 500000 500000 0 15 32 65535 4000 4000
```

Where:

- For the **cnfcdsct 4** command, 4 = policing on; 5 = policing off (for ATMF service types).

- The **upln 1.1** command brings up the line where you want to add the port.
- The **addport** command adds the port. The syntax for the command is as follows:

addport *ifNum bay.line guaranteedRate maxRate sctID ifType [vpiNum]*

Where:

ifNum is a number between 1 and 60
bay.line is the format for the Line Number
guaranteedRate is the virtual rates in cells/sec
maxRate for OC48 = between 50 and 5651320
 for OC12 = between 50 and 1412830
 for OC3 = between 50 and 353207
 for T3 = between 50 and 96000 (PLCP), 104268 (ADM)
 for E3 = between 50 and 80000
sctID is the Port SCT ID between 0 and 255, for the default file use 0
ifType is 1 for UNI; 2 for NNI; 3 for VNNI
vpiNum is between 1 and 4095, used for configuring the interface as virtual trunk

The *guaranteedRate* argument must equal the *maxRate* argument.

- The **addpart** command partitions the port you just added. The syntax for the command is as follows:

addpart *ifNum partID cntlrID egrminbw egrmaxbw ingrminbw ingrmaxbw minVpi maxVpi minVci maxVci minConns maxConns*

Where:

ifNum is a number between 1 and 60
partID is the partition identifier between 1 and 20
cntlrID is the controller identifier between 1 and 20
egrminbw is the Egress guaranteed percentage of bandwidth in units of 0.0001% of interface bandwidth
egrmaxbw is the Egress maximum percentage of bandwidth in units of 0.0001% of interface bandwidth
ingrminbw is the Ingress guaranteed percentage of bandwidth in units of 0.0001% of interface bandwidth
ingrmaxbw is the Ingress maximum percentage of bandwidth in units of 0.0001% of interface bandwidth
minVpi is the minimum VPI value, which is a number between 0 and 4095 (0 to 255 for the UNI interface)
maxVpi is the maximum VPI value, which is number between 0 and 4095 (0 to 255 for the UNI interface)
minVci is the minimum VCI value, which is a number between 32 and 65535
maxVci is the maximum VCI value, which is a number between 32 and 65535
minConns is the guaranteed number of connections, which is a number between 0 and the maximum number of connections in portgroup (see **dspscd** for portgroup info)
maxConns is the maximum number of connections, which is a number between 0 and the maximum number of connections in portgroup (see **dspscd** for portgroup info)

- The **dspparts** command displays the newly added partition and verifies its settings.

Configuration for BXP

BPX:

```
uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3
cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000
```

Configuration for Cisco 7200 LSC

7200 LSC:

```

ip cef
!
mpls atm disable-headend-vc
!
interface loopback0
    ip address 40.40.40.40 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
    extended-port ATM3/0 bpx 1.3
    ip unnumbered loopback0
    mpls atm vpi 2-15
    mpls ip
!
interface XTagATM22
    extended-port ATM3/0 bpx 2.2
    ip unnumbered loopback0
    mpls atm vpi 2-5
    mpls ip
!
router ospf 100
    network 40.0.0.0 0.255.255.255 area 0

```

Configuration for Cisco 7200 Edge LSR2

7200 LSR2:

```

ip cef
!
interface loopback 0
    ip address 30.30.30.30 255.255.255.255
!
interface ATM2/0/0
    no ip address
!
interface ATM2/0/0.5 mpls
    ip unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip
!
router ospf 100
    network 30.0.0.0 0.255.255.255 area 0

```

PVP-Based ATM MPLS Network Configuration

This section contains sample configurations for the following PVP-based ATM MPLS network configurations:

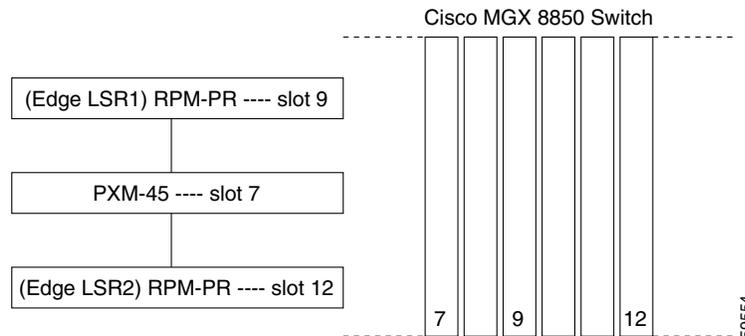
- [Edge LSR to Edge LSR SPVP LC-ATM Interface Configuration, page 39](#)
- [Cisco MGX 8850 RPM-PR Connected to an External Device, page 42](#)

Edge LSR to Edge LSR SPVP LC-ATM Interface Configuration

Figure 8 represents a sample permanent virtual path (PVP) configuration with devices in the same Cisco MGX 8850 switch for the ATM MPLS network configuration examples that follow.

- [RPM-PR Edge LSR1 Configuration with VPC Switch Partition, page 39](#)
- [PXM-45 Configuration with VPC Switch Partition, page 40](#)
- [RPM -PR Edge LSR2 Configuration with VPC Switch Partition, page 41](#)

Figure 8 PVP Configuration with Devices in Same Cisco MGX 8850 Switch



Note

If two RPM-PRs in adjacent slots share the same cellbus, you need to configure a clock rate of 42 MHz on the PXM-45. Use the **dspeblk** command to display the clock rate. Use the **cnfcbclk cbn 42** command to change the clock rate, where *n* is the number of the cellbus.

RPM-PR Edge LSR1 Configuration with VPC Switch Partition

This example uses the **switch partition vpc** command and therefore, you can use VPI ranges or VP tunnels. If you create a VP tunnel between two routers, you need to configure VPC partitioning and PNNI signaling to bring up the PVP. Then you can run the LC-ATM interface on the PVP.



Note

In the Cisco MGX 8850 switch, the partition resources of the switch ports are configured at the RPM-PR. In the Cisco BPX switch, you configure all resources in the switch.

Following is a sample configuration for the RPM-PR Edge LSR1:

```
ip cef
!
interface Loopback0
 ip address 10.9.9.9 255.255.255.255
!
interface Switch1
 atm pvp 2 10000
 switch partition vpc 1 2
 ingress-percentage-bandwidth 1 100
 egress-percentage-bandwidth 1 100
 vpi 1 255
 vci 0 65535
!
interface Switch1.2 mpls
 ip unnumbered Loopback0
 pvc 2/0
 mpls atm control-vc 2 32
```

```

mpls atm vpi 2 vci 33-65518
mpls ip
switch connection vpc 2 master remote
!
router ospf 100
network 10.0.0.0 0.255.255.255 area 0

```

Where:

- The **switch partition vpc 1 2** command configures the VPC switch partition. For PNNI, the partition ID = 1 and the controller ID = 2.
- The **ingress-percentage-bandwidth 1 100** partition resource command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.
- In the **interface Switch1.2 mpls** command, the interface is Switch1.2.
- The **pvc 2/0** command configures a PVC = 2/0 on the VP.
- The **switch connection vpc 2 master remote** command enables PNNI to create a PVP (VPI = 2) connection. This command also indicates that the remote peer is the master, therefore, this is slave side.



Note You need to configure the slave side first. Then, you are able to get the ATM NSAP address from the PXM. This is needed at the master side.

PXM-45 Configuration with VPC Switch Partition

This illustrates the PXM configuration for VPC switch partitioning for a PVP when all devices exist on the same Cisco MGX 8850 switch.

At the PXM-45 SWITCH.7.PXM.a> prompt:

```

addcontroller 2 i 2 7 PNNI
dnpport 9.2
cnfpnportsig 9.2 -univer none
uppport 9.2
dspcon 9.2 2

```

Port	Vpi Vci	Owner	State
Local 9:-1.2:-1	2.0	SLAVE	FAIL
Address: 47.009181000000000142265fb2.000001074b02.00			
Node name: SWITCH			
Remote Routed	0.0	MASTER	--
Address: 00.000000000000000000000000.000000000000.00			
Node name:			

```

----- Provisioning Parameters -----
Connection Type: VPC                               Cast Type: Point-to-Point
Service Category: UBR                               Conformance: UBR.1
Bearer Class: BCOB-VP
Last Fail Cause: N/A                               Attempts: 0
Continuity Check: Disabled                          Frame Discard: Disabled
L-Utils: 0 R-Utils: 0 Max Cost: 0 Routing Cost: 0
OAM Segment Ep: Enabled
----- Traffic Parameters -----
Tx PCR: 353208 Rx PCR: 353208
Tx CDV: N/A Rx CDV: N/A
Tx CTD: N/A Rx CTD: N/A

```

Where:

- The **dnpport** command brings down the port so that it can be configured. In this example, the **dnpport 9.2** command indicates slot 9 and the VPC partition.



Note In the **dsppport** *port_id* command, the *port_id = slot#.part*, where *part* options are 1 = VCC; 2 = VPC.

- The **cnfnpportsig 9.2 -univer none** command disables PNNI signaling on the RPM-PR is in slot 9.
- The **uppport** command brings up the ports after configuration is complete.
- After configuring **switch connection vpc 2 master remote** on slave (Edge LSR1), you use the **dspcon** command on the PXM to get the slave NSAP address. In the **dspcon 9.2 2** command, the final 2 is the VPC value.

RPM -PR Edge LSR2 Configuration with VPC Switch Partition

This example uses the **switch partition vpc** command and therefore, you can use VPI ranges or VP tunnels. If you create a VP tunnel between two routers, you need to configure VPC partitioning and PNNI signaling to bring up the PVP. Then you can run the LC-ATM interface on the PVP.



Note

In the Cisco MGX 8850 switch, the partition resources of the switch ports are configured at the RPM-PR. In the Cisco BPX switch, you configure all resources in the switch.

Following is a sample configuration for the RPM-PR Edge LSR2:

```
ip cef
!
interface Loopback0
 ip address 12.12.12.12 255.255.255.255
!
interface Switch1
 atm pvp 2 10000
 switch partition vpc 1 2
 ingress-percentage-bandwidth 1 100
 egress-percentage-bandwidth 1 100
 vpi 1 255
 vci 0 65535
!
interface Switch1.2 mpls
 ip unnumbered Loopback0
 pvc 2/0
 mpls atm control-vc 2 32
 mpls atm vpi 2 vci 33-65518
 mpls ip
 switch connection vpc 2 master local raddr
 47.0091.8100.0000.0001.4226.5fb2.0000.0107.4b02.00 2
!
!router ospf 100
 network 12.0.0.0 0.255.255.255 area 0
!
dspcon 9.2 2
```

Port	Vpi Vci	Owner	State
Local 9:-1.2:-1	2.0	SLAVE	OK
Address: 47.009181000000000142265fb2.000001074b02.00			
Node name: SWITCH			
Remote Routed	0.0	MASTER	OK
Address: 47.009181000000000142265fb2.000001076302.00			

```

Node name:
----- Provisioning Parameters -----
Connection Type: VPC           Cast Type: Point-to-Point
Service Category: UBR         Conformance: UBR.1
Bearer Class: BCOB-VP
Last Fail Cause: No Fail      Attempts: 0
Continuity Check: Disabled    Frame Discard: Disabled
L-Utills: 100   R-Utills: 100   Max Cost: -1   Routing Cost: 0
OAM Segment Ep: Enabled
----- Traffic Parameters -----
Tx PCR: 353208      Rx PCR: 353208
Tx CDV: N/A        Rx CDV: N/A
Tx CTD: N/A        Rx CTD: N/A

```

Where:

- The 1,100 in the **ingress-percentage-bandwidth 1 100** command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.
- The NSAP ATM address for the switch connection command is found by entering the **dspon** command on the PXM-45 card.
- Executing the **dspon 9.2 2** command, for example, at the end of the configuration should show both local (slave) and remote (master) addresses.

PXM-45 Configuration with VPC Switch Partition

This illustrates the PXM configuration for VPC switch partitioning for a PVP when all devices exist on the same Cisco MGX 8850 switch.

At the PXM-45 SWITCH.7.PXM.a> prompt:

```

dnpport 12.2
cnfportsig 12.2 -univer none
uppport 12.2

```

Where:

- The **dnpport** command brings down the port so that it can be configured. In this example, the **dnpport 12.2** command brings down port 12 and the VPC partition.



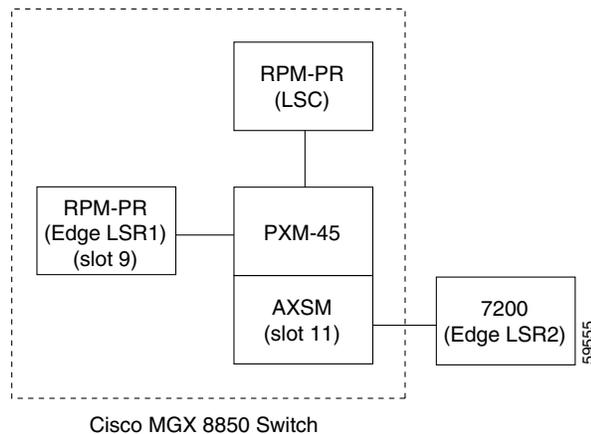
Note In the **dsppnport port_id** command, the *port_id = slot#.part*, where *part* options are 1 = VCC; 2 = VPC.

- The **cnfportsig 12.2 -univer none** command disables PNNI signaling for the RPM-PR in slot 12.
- The **uppport** command brings up the ports after configuration is complete.

Cisco MGX 8850 RPM-PR Connected to an External Device

These sample configurations illustrate a permanent virtual path (PVP) ATM MPLS network with the Cisco MGX 8850 RPM-PR in the Cisco MGX 8850 switch connected to an external device (a Cisco 7200 router, for example). [Figure 9](#) illustrates a PVP configuration with the RPM-PR in the Cisco MGX 8850 switch connected to a Cisco 7200 Edge LSR for the configuration examples that follow.

- [RPM-PR Edge LSR1 Configuration \(VPC Switch Partition\), page 43](#)
- [PXM-45 Configuration \(Switch Partition VPC\), page 44](#)
- [Configuration for Cisco 7200 Edge LSR2, page 46](#)

Figure 9 RPM-PR in Cisco MGX 8850 Switch Connected to Cisco 7200 Edge LSR**Note**

If two RPM-PRs in adjacent slots share the same cellbus, you need to configure a clock rate of 42 MHz on the PXM-45. Use the **dspeblk** command to display the clock rate. Use the **cnfcbclk cbn 42** command to change the clock rate, where **n** is the number of the cellbus.

These examples use the **switch partition vpc** command and therefore, you can use VPI ranges or VP tunnels. If you create a VP tunnel between two routers, you need to configure VPC partitioning and PNNI signaling to bring up the PVP. Then you can run the LC-ATM interface on the PVP.

Between Cisco MGX 8850 RPM-PRs, you can use signaled connections, soft permanent virtual circuit (SPVC) and soft permanent virtual path (SPVP) connections, using PNNI. For this type of connection with VPC partitions, you can use any VPI = 1 to 256. You can run MPLS on SPVCs or SPVPs. With MPLS, you can configure the following:

- On the SPVCs—Packet MPLS Downstream Unsolicited TDP or LDP
- On the SPVPs—LC-ATM Downstream on Demand TDP or LDP

If you are connecting the Cisco RPM-PR Edge LSR with other routers, such as the Cisco 7200 router, the Cisco 12000 router, or the Cisco BPX or Cisco IGX switch with the Cisco 7200 router, then you need to connect these routers through AXSM or AXSM-E cards. The Cisco 7200, and Cisco 12000 routers, and the Cisco BPX or Cisco IGX switch with the Cisco 7200 router cannot use PNNI signaling. You need to do the following:

- Start the SPVCs and SPVPs from the RPM-PR and terminate them in the AXSM or AXSM-E cards. (PNNI signaling makes the connection between the RPM-PR and the AXSM or AXSM-E cards.)
- Provision the PVC and PVP connections manually at the Cisco 7200, and Cisco 12000 routers, and the Cisco BPX or Cisco IGX switch with the Cisco 7200 router.

RPM-PR Edge LSR1 Configuration (VPC Switch Partition)

```

ip cef
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
!
interface Switch1
 atm pvp 12 100000
 switch partition vpc 1 2
 ingress-percentage-bandwidth 20 100
 egress-percentage-bandwidth 20 100
  
```

```

vpi 1 100
vci 0 65535
!
interface Switch1.12 mpls
 ip unnumbered Loopback0
 pvc 12/0
 ubr 100000
 mpls atm vp-tunnel 12 vci-range 33-65518
 mpls ip
 switch connection vpc 12 master remote
!
router ospf 100
 network 12.0.0.0 0.255.255.255 area 0

```

Where:

- The **atm pvp 12 100000** command configures a PVP with PCR = 100000 Kbps. You calculate the AXSM endpoints = about 235900 based on this value of 100000 Kbps ((100000 x 1000) divided by (53 x 8)).
- In the **pvc 12/0** command, the PVC should be the VPI of the SPVP and a VCI = 0.
- The **switch connection vpc 12 master remote** command enables PNNI to set up SPVP 12.

PXM-45 Configuration (Switch Partition VPC)

The following examples show PVP-based ATM MPLS network configurations for the AXSM and PXM-45 cards.

At the AXSM SWITCH.11.AXSM.a> prompt:

```

upln 1.2
addport 2 1.2 40000 40000 4 2
addpart 2 1 2 235900 235900 235900 235900 1 100 32 65535 10 100

```

At the PXM-45 SWITCH.7.PXM.a> prompt:

```

addcontroller 2 i 27 PNNI
dnport 9.2
cnfpnportsig 9.2 -univer none
uppnport 9.2
!
dspports

```

ifNum	Line	Admin State	Oper. State	Guaranteed Rate	Maximum Rate	Port VNNI only)	SCT Id	ifType	VPI
1	1.1	Up	Down	353207	353207	5		UNI	0
2	1.2	Up	Up	40000	40000	4		NNI	0

At the AXSM SWITCH.11.AXSM.a> prompt:

```

dspport 2

Interface Number      : 2
Line Number           : 1.2
Admin State           : Up      Operational State    : Up
Guaranteed bandwidth(cells/sec): 40000      Number of partitions: 1
Maximum bandwidth(cells/sec) : 40000      Number of SPVC      : 0
ifType                : NNI          Number of SPVP      : 0
Port SCT Id           : 4
VPI number(VNNI only) : 0          Number of SVC       : 0

dspport 1

```

```

Interface Number      : 1
  Line Number         : 1.1
  Admin State         : Up           Operational State : Down
  Guaranteed bandwidth(cells/sec): 353207   Number of partitions: 1
  Maximum bandwidth(cells/sec)   : 353207   Number of SPVC      : 0
  ifType              : UNI           Number of SPVP      : 0
  Port SCT Id         : 5
  VPI number(VNNI only) : 0           Number of SVC       : 0

```

```
dsppart 2 1
```

```

Interface Number      : 2
  Partition Id        : 1           Number of SPVC: 0
  Controller Id       : 2           Number of SPVP: 0
  egr Guaranteed bw(.0001percent): 1000000   Number of SVC : 0
  egr Maximum bw(.0001percent)   : 1000000
  ing Guaranteed bw(.0001percent): 1000000
  ing Maximum bw(.0001percent)   : 1000000
  min vpi              : 1
  max vpi              : 100
  min vci              : 32
  max vci              : 65535
  guaranteed connections : 10
  maximum connections   : 100

```

At the PXM-45 SWITCH.7.PXM.a> prompt:

```
dspscons
```

Local Port	Vpi.Vci	remote Port	Vpi.Vci	State	Owner
9.1	0 2000	12.1	0 2000	OK	SLAVE
Local Addr: 47.0091810000000000142265fb2.0000001074b01.00					
Remote Addr: 47.0091810000000000142265fb2.0000001076301.00					
12.1	0 2000	9.1	0 2000	OK	MASTER
Local Addr: 47.0091810000000000142265fb2.0000001076301.00					
Remote Addr: 47.0091810000000000142265fb2.0000001074b01.00					
12.2	12 0	Routed	0 0	FAIL	SLAVE
Local Addr: 47.0091810000000000142265fb2.0000001076302.00					
Remote Addr: 00.0000000000000000000000000000000000.000000000000.00					

At the AXSM SWITCH.11.AXSM.a> prompt:

```

addcon 2 12 0 8 1 -slave 470091810000000000142265fb200000107630200.12.0 -lpcr
8000 -rpcr 8000
master endpoint added successfully
master endpoint id : 470091810000000000142265FB20000010B180200.12.0

```

At the PXM-45 SWITCH.7.PXM.a> prompt:

```
dspscons
```

Local Port	Vpi.Vci	Remote Port	Vpi.Vci	State	Owner
9.1	0 2000	12.1	0 2000	OK	SLAVE
Local Addr: 47.0091810000000000142265fb2.0000001074b01.00					
Remote Addr: 47.0091810000000000142265fb2.0000001076301.00					
12.1	0 2000	9.1	0 2000	OK	MASTER
Local Addr: 47.0091810000000000142265fb2.0000001076301.00					
Remote Addr: 47.0091810000000000142265fb2.0000001074b01.00					
12.2	12 0	11:1.2:2	12 0	OK	SLAVE
Local Addr: 47.0091810000000000142265fb2.0000001076302.00					
Remote Addr: 47.0091810000000000142265fb2.00000010b1802.00					
11:1.2:2	12 0	12.2	12 0	OK	MASTER

```
Local Addr: 47.009181000000000142265fb2.0000010b1802.00
Remote Addr: 47.009181000000000142265fb2.000001076302.00
master endpoint id : 47009181000000000142265FB20000010B180200.12.0
```

Where:

- The **cnfnpnportsig 9.2 -univer none** command configures the signaling for the RPM-PR's switch interface 1.12.

Configuration for Cisco 7200 Edge LSR2

```
ip cef
!
interface loopback 0
    ip address 10.9.9.9 255.255.255.255
!
interface ATM2/0
    no ip address
!
interface ATM2/0.9 mpls
    ip unnumbered loopback 0
    mpls atm vpi 12
    mpls ip
!
router ospf 100
    network 10.0.0.0 0.255.255.255 area 0
```

PXM-45 Configuration with VPC Switch Partition

At the PXM-45 SWITCH.7.PXM.a> prompt:

```
dnport 11:1.2:2
cnfnpnportsig 11:1.2:2 -univer none
uppnport 11:1.2:2
```

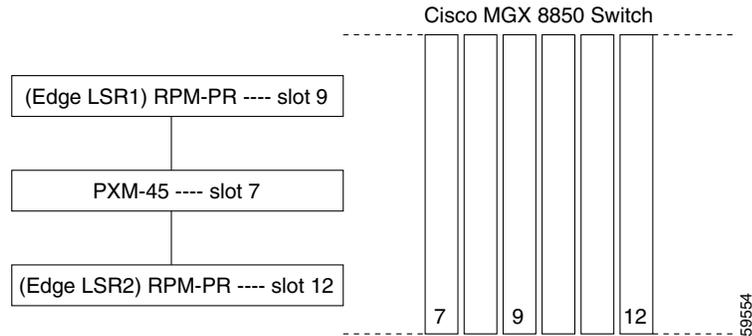
Where:

- The **cnfnpnportsig 11:1.2:2 -univer none** command configures the signaling for the AXSM at slot 11 and line 1.2.

Simple PVC-Based Packet MPLS Network Configuration

This section contains configuration examples for a simple permanent virtual circuit (PVC) packet MPLS network. For this example all devices are in the same Cisco MGX 8850 switch. [Figure 10](#) illustrates a PVC packet MPLS network with all devices in the same Cisco MGX 8850 switch.

- [RPM-PR Edge LSR1 Configuration \(Switch Partition VCC\), page 47](#)
- [PXM-45 Configuration \(Switch Partition VCC\), page 48](#)
- [RPM-PR Edge LSR2 Configuration \(Switch Partition VCC\), page 48](#)

Figure 10 PVC Packet MPLS Network with All Devices in the Same Cisco MGX 8850 Switch**Note**

If two RPM-PRs in adjacent slots share the same cellbus, you need to configure a clock rate of 42 MHz on the PXM-45. Use the **dspcbclk** command to display the clock rate. Use the **cnfcbclk cbn 42** command to change the clock rate, where *n* is the number of the cellbus.

RPM-PR Edge LSR1 Configuration (Switch Partition VCC)

This example uses the **switch partition vcc** command and therefore, you can use only VCI ranges; you cannot use VPI ranges or VP tunnels. To create and bring up a PVC between two routers, you need to configure VCC partitioning and PNNI signaling. Then you can run packet-based MPLS for the PVC.

**Note**

In the Cisco BPX or IGX switches, all resources are configured in the switch.

```

ip cef
!
interface Loopback0
 ip address 9.9.9.9 255.255.255.255
!
interface Switch1
 switch partition vcc 1 2
 ingress-percentage-bandwidth 1 100
 egress-percentage-bandwidth 1 100
 vpi 0 0
 vci 32 3808
!
interface Switch1.2 point-to-point
 ip unnumbered Loopback0
 pvc 0/2000
 oam-pvc manage
 encapsulation aal5snap
!
mpls ip
 switch connection vcc 0 2000 master remote
!
router ospf 100
 network 9.0.0.0 0.255.255.255 area 0

```

Where:

- The **switch partition vcc 1 2** command configures the VCC switch partition. The PNNI partition ID = 1 and the PNNI controller ID = 2.

- The 1, 100 in the **ingress-percentage-bandwidth 1 100** command guarantees 1 percent of the bandwidth to that partition. The partition can use up to 100 percent of the bandwidth.
- In the **interface Switch1.2 point-to-point** command, the interface is 1.2.
- The **oam-pvc manage** command configures Operation, Administration, and Maintenance (OAM) to check the end-to-end PVC link status.
- The **switch connection vcc 0 2000 master remote** command enables PNNI and makes the PVC (VPI=0, VCI=2000) connection. The command indicates that the remote peer is the master. You are on the slave side. You need to configure the slave side first. Then you can get the ATM NSAP address from the PXM that is required at the master side.

PXM-45 Configuration (Switch Partition VCC)

This example shows commands to configure the PXM-45 for a simple PVC packet MPLS network.

At the PXM-45 SWITCH.7.PXM.a> prompt:

```
addcontroller 2 i 2 7 PNNI
dnpport 9.1
cnfnpportsig 9.1 -univer none
uppport 9.1

dspcon 9.2 1
```

Where:

- The **dnpport 9.1** command brings the port down for configuration. The 9.1 indicates slot 9 and the VCC (1) partition.
- The **cnfnpportsig 9.1 -univer none** command disables PNNI signaling for the RPM-PR in slot 9.
- The **uppport** command brings the port back up.
- After configuring **switch connection vcc 0 2000 master remote** on the slave (Edge LSR1), use the **dspcon** command on the PXM-45 to get the slave NSAP address.
- In the **dspcon 9.2 1** command, the 1 is the VCC value.

RPM-PR Edge LSR2 Configuration (Switch Partition VCC)

This example uses the **switch partition vcc** command and therefore, you can use only VCI ranges; you cannot use VPI ranges or VP tunnels. To create and bring up a PVC between two routers, you need to configure VCC partitioning and PNNI signaling. Then you can run packet-based MPLS for the PVC.

```
ip cef
!
interface Loopback0
 ip address 12.12.12.12 255.255.255.255
!
interface Switch1
 switch partition vcc 1 2
 ingress-percentage-bandwidth 1 100
 egress-percentage-bandwidth 1 100
 vpi 0 0
 vci 1501 3808
!
interface Switch1.2 point-to-point
 ip unnumbered Loopback0
 pvc 0/2000
 oam-pvc manage
 encapsulation aal5snap
!
```

```

mpls ip
  switch connection vcc 0 2000 master local raddr
    47.0091.8100.0000.0001.4226.5fb2.0000.0107.4b01.00 0 2000
!
router ospf 100
  network 12.0.0.0 0.255.255.255 area 0

```

Where:

- The **switch partition vcc 1 2** command configures the VCC switch partition. The PNNI partition ID = 1 and the PNNI controller ID = 2.
- The **oam-pvc manage** command configures Operation, Administration, and Maintenance (OAM) to check the end-to-end PVC link status.
- The **mpls ip** command enables packet-based MPLS on the PVC.
- In the command **switch connection vcc 0 2000 master local raddr 47.0091.8100.0000.0001.4226.5fb2.0000.0107.4b01.00 0 2000**, the NSAP ATM address is retrieved from the PXM-45 switch, using the **dspecon** command.

PXM-45 Configuration (Switch Partition VCC)

This example shows commands to configure the PXM-45 for a simple PVC packet MPLS network.

At the PXM-45 SWITCH.7.PXM.a> prompt:

```

addcontroller 2 i 2 7 PNNI
dnpport 12.1
cnfnpportsig 12.1 -univer none
uppport 12.1

```

Where:

- The **dnpport 12.1** command brings the port down for configuration. The 12.1 indicates slot 12 and the VCC (1) partition.
- The **cnfnpportsig 12.2 -univer none** command disables PNNI for the RPM-PR is in slot 12.
- The **uppport** command brings the port back up.

Configuring the Cisco 6400 Universal Access Concentrator as an MPLS LSC

You can configure the Cisco 6400 Universal Access Concentrator (UAC) to operate as an MPLS LSC in an MPLS network. The hardware that supports MPLS LSC functionality on the Cisco 6400 UAC is described in the following sections.



Note

If you configure a Cisco 6400 UAC with a node resource processor (NRP) to function as an LSC, disable MPLS Edge LSR functionality. Refer to the command **mpls atm disable-headend-vc** for information on disabling MPLS Edge LSR functionality. An NRP LSC should support transit label switch paths only through the controlled ATM switch under VSI control.

Cisco 6400 UAC Architectural Overview

A Cisco 6400 UAC can operate as an MPLS LSC if it incorporates the following components:

- Node switch processor (NSP)—The NSP incorporates an ATM switch fabric, enabling the Cisco 6400 UAC to function as an ATM label switch router (ATM LSR) in a network. The NSP manages all the external ATM interfaces for the Cisco 6400 UAC.
- Node route processor (NRP)—The NRP enables a Cisco 6400 UAC to function as an LSC. When you use the NRP as an LSC, however, you must not configure the NRP to perform other functions. The NRP contains internal ATM interfaces that enable it to be connected to the NSP. However, the NRP cannot access the external ATM interfaces of the Cisco 6400 UAC. Only the NSP can access the external ATM interfaces.

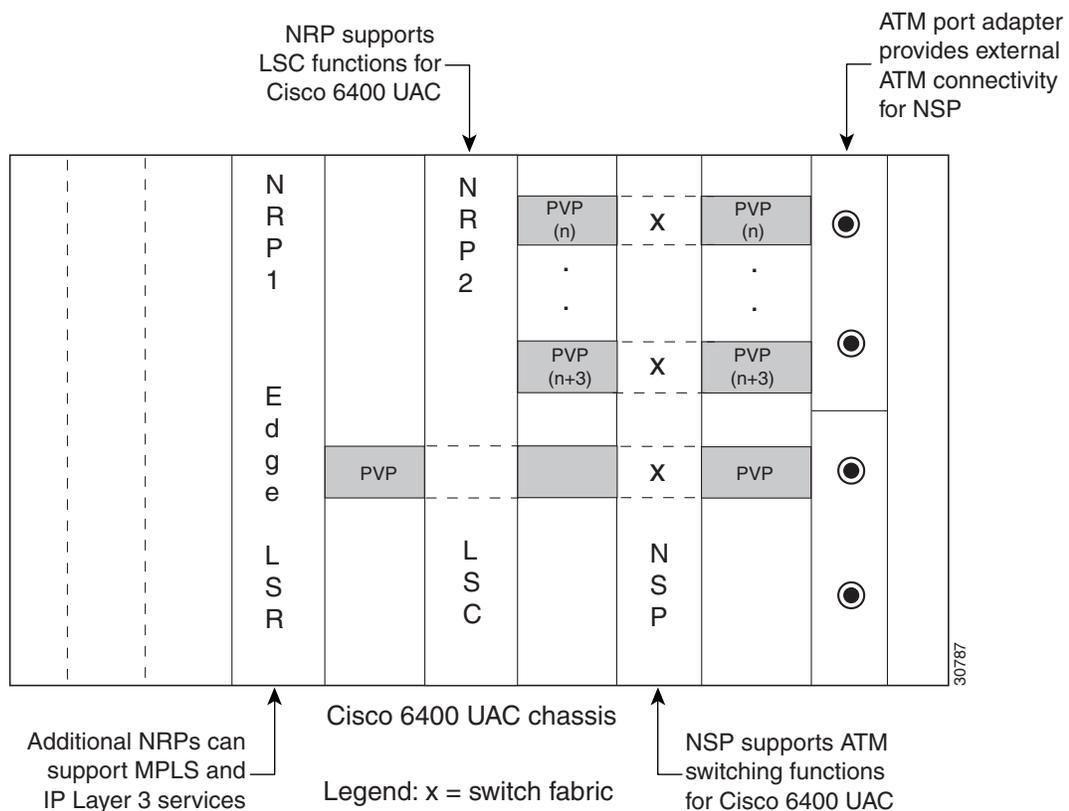


Note A Cisco 6400 UAC chassis can accommodate multiple NRPs, including one dedicated to MPLS LSC functions. You cannot use an additional NRP as an MPLS LSC. However, you can use additional NRPs to run MPLS and perform other networking services.

- ATM port adapter—The Cisco 6400 UAC uses an ATM port adapter to provide external connectivity for the NSP.

Figure 11 shows the components that you can configure to enable the Cisco 6400 UAC to function as an MPLS LSC.

Figure 11 Cisco 6400 UAC Configured as an MPLS LSC



Configuring Permanent Virtual Circuits and Permanent Virtual Paths

The NRP controls the slave ATM switch through the Virtual Switch Interface (VSI) protocol. The VSI protocol operates over a permanent virtual circuit (PVC) that you configure. The PVC is dedicated to the virtual circuits (VCs) that the VSI control channel uses.

For the NRP to control an ATM switch through the VSI, cross-connect the control VCs from the ATM switch through the NSP to the NRP. The ATM switch uses defined control VCs for each BXM slot of the BPX chassis, enabling the LSC to control external XTagATM interfaces through the VSI.

[Table 5](#) defines the PVCs that must be configured on the NSP interface connected to the BPX VSI shelf. These PVCs are cross-connected via the NSP to the NRP VSI master control port, which is running the VSI protocol.

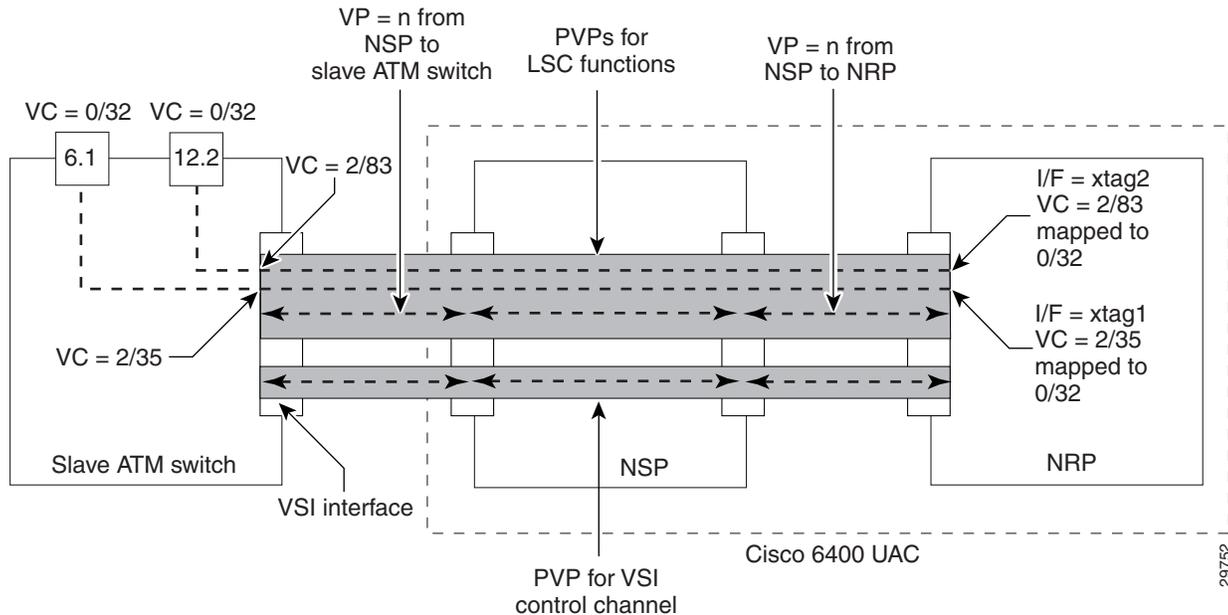
For an NRP that is installed in slot 3 of a Cisco 6400 UAC chassis, the master control port would be ATM3/0/0 on the NSP. As shown in [Figure 2](#), the BPX switch control interface is 12.1. The NSP ATM port connected to interface 12.1 is the ATM interface that is cross-connected to ATM3/0/0. [Figure 2](#) shows that the BXM slaves in BPX slots 6 and 12 are configured as external XTagATM ports. The PVCs that must be cross-connected through the NSP are 0/45 for slot 6 and 0/51 for slot 12, respectively, as outlined in [Table 5](#).

Table 5 VSI Interface Control PVCs for BPX VSI Slave Slots

BPX VSI Slave Slot	VSI Interface Control VC
1	0/40
2	0/41
3	0/42
4	0/43
5	0/44
6	0/45
7	0/46
8	0/47
9	0/48
10	0/49
11	0/50
12	0/51
13	0/52
14	0/53

[Figure 12](#) shows the functional relationships among the Cisco 6400 UAC hardware components and the permanent virtual paths (PVPs) that you can configure to support MPLS LSC functionality.

Figure 12 Cisco 6400 UAC PVP Configuration for MPLS LSC Functions



All other MPLS LSC functions, such as routing, terminating LVCs, and LDP control VCs (default 0/32), can be accomplished by means of a separate, manually configured PVP (see the upper shaded area in Figure 12). The value of “n” for this manually configured PVP must be the same among all the associated devices (the NRP, the NSP, and the slave ATM switch). Because the NSP uses VP=0 for ATM Forum signaling and the BPX uses VP=1 for autoroute, the value of “n” for this PVP for MPLS LSC functions must be greater than or equal to 2, while not exceeding an upper bound.

Note that some Edge LSRs have ATM interfaces with limited VC space per virtual path (VP). For these interface types, you define several VPs. For example, the Cisco ATM Port Adapter (PA-A1) and the AIP interface are limited to VC range 33 through 1018. To use the full capacity of the ATM interface, configure four consecutive VPs. Make sure the VPs are within the configured range of the BPX.

For internodal BPX connections, it is suggested that you configure VPs 2 through 15; for Edge LSRs, it is suggested that you configure VPs 2 through 5. (See the IOS CLI command `mpls atm vpi` for examples of how to configure Edge LSRs; see the BPX command “`cnfrsrc`” described in the *Cisco BPX 8600 Series* documentation for examples of how to configure BPX service nodes.)

Control VC Setup for MPLS LSC Functions

After you connect the NRP, the NSP, and the slave ATM switch by means of manually configured PVPs (as shown in Figure 12), the NRP can control the slave ATM switch as though it is directly connected to the NRP. The NRP discovers the interfaces of the slave ATM switch and establishes the default control VC to be used in creating MPLS VCs.

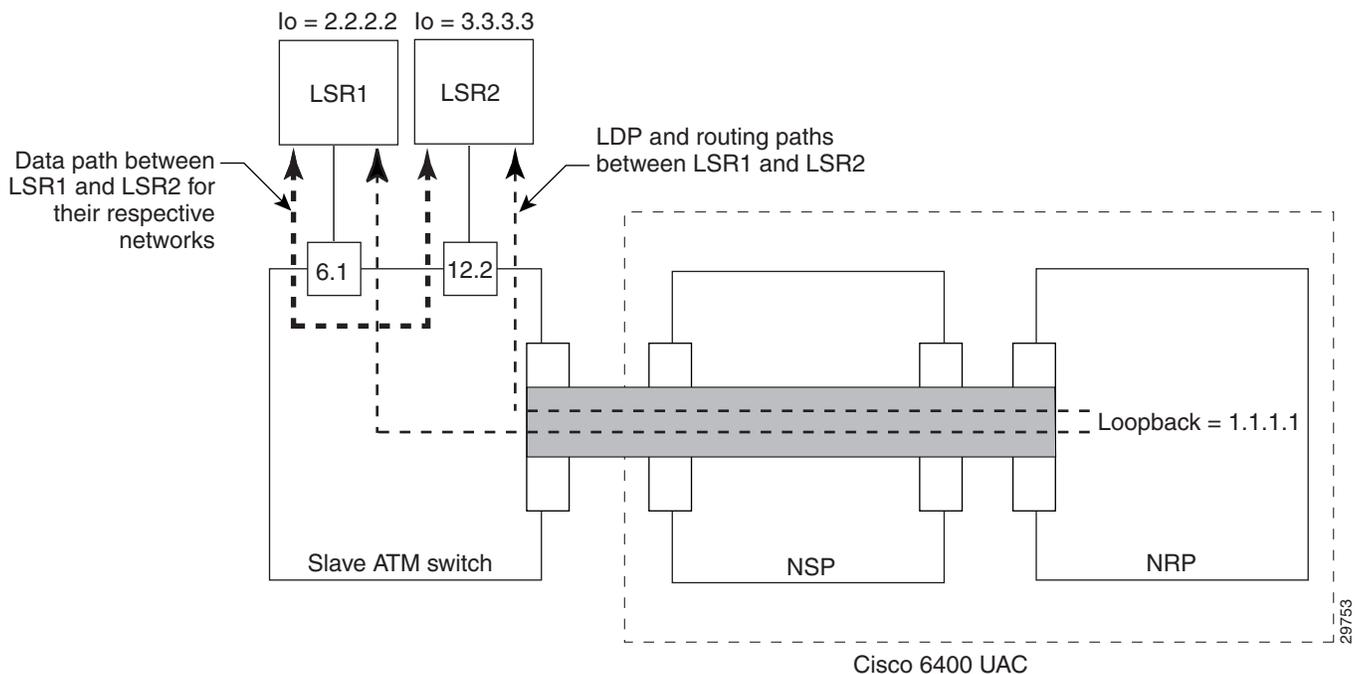
The slave ATM switch shown in Figure 12 incorporates two external ATM interfaces (labeled 1 and 2) that are known to the NRP as XTagATM61 and XTagATM122, respectively. On interface 6.1 of the slave ATM switch, VC 0/32 is connected to VC 2/35 by the VSI protocol. On the NRP, VC 2/35 is terminated on interface XTagATM61 and mapped to VC 0/32, also by means of the VSI protocol. This mapping enables the LDP to discover MPLS LSC neighbors by means of the default control VC 0/32 on the physical interface. On interface 12.2 of the slave ATM switch, VC 0/32 is connected to VC 2/83 by the VSI protocol. On the NRP, VC 2/83 is terminated on interface XTagATM122 and mapped to VC 0/32.

Note that the selection of these VCs depends on the availability of VC space. Hence it is not predictable what physical VC will be mapped to the external default control VC 0/32 on the XTagATM interface. The control VC is shown as a PVC on the LSC, as opposed to a LVC, when you execute the IOS CLI command `show xtagatm vc`.

Configuring the Cisco 6400 UAC to Perform Basic MPLS LSC Operations

Figure 13 shows a Cisco 6400 UAC containing a single NRP that has been configured to perform basic MPLS LSC operations.

Figure 13 Typical Cisco 6400 UAC Configuration to Support MPLS LSC Functions



Note

If the NRP incurs a fault that causes it to malfunction (in a single NRP configuration), the LVCs and routing paths pertaining to MPLS LSC functions are lost.



Note

The loopback addresses must be configured with a 32-bit mask and be included in the relevant IGP or BGP routing protocol, as shown in the following example:

```
ip address 172.103.210.5 255.255.255.255
```

Defining the MPLS Control and IP Routing Paths

In the MPLS LSC topology shown in Figure 13, the devices labeled LSR1 and LSR2 are external to the Cisco 6400 UAC. These devices, with loopback addresses as their respective LDP identifiers, are connected to two separate interfaces labeled 6.1 and 12.2 on the slave ATM switch. Both LSR1 and LSR2

learn about each other's routes from the NRP by means of the data path represented as the thick dashed line in [Figure 13](#). Subsequently, LVCs are established by means of LDP operations to create the data paths between LSR1 and LSR2 through the ATM slave switch.

Both LSR1 and LSR2 learn of the loopback address of the NRP and create a data path (LVCs) from each other that terminates in the NRP. These LVCs, called tailend LVCs, are not shown in [Figure 13](#).

Disabling Edge LVCs

By default, the NRP requests LVCs for the next hop devices (the LSRs shown in [Figure 13](#)). The headend LVCs enable the LSC to operate as an edge LSR. Using the LSC as an edge LSR is not supported. Further, the NRP is dedicated to control the slave ATM switch. Therefore, the headend LVCs are not required.

If a Cisco 6400 UAC with an NRP is configured to function as an LSC, disable the edge LSR functionality. An NRP LSC should support transit label switch paths only through the ATM switch using the VSI protocol. To disable the LSC from acting as an edge LSR, see [“Disabling the LSC from Acting as an Edge LSR” section on page 63](#).

Configuration Steps: Configuring Cisco 6400 UAC NRP as an MPLS LSC

To configure the Cisco 6400 UAC NRP as an MPLS LSC, perform the following steps:

	Command	Purpose
Step 1	<pre>Router(config)# interface loopback0 Router(config-if)# ip address 172.103.210.5 255.255.255.255 Router(config-if)# exit</pre>	<p>Creates a software-only loopback interface that emulates an interface that is always up. Specify an interface number for the loopback interface. There is no limit on the number of loopback interfaces you can create.</p> <p>Assigns an IP address to Loopback0. It is important that all loopback addresses in an MPLS network are host addresses, that is, with a mask of 255.255.255.255. Using a shorter mask can prevent MPLS-based VPN services from working correctly.</p>
Step 2	<pre>Router(config)# interface atm1/0/0 Router(config-if)# tag-control-protocol vsi Router(config-if)# ip route-cache cef</pre>	<p>Creates an ATM interface (atm1/0/0).</p> <p>Enables the VSI protocol on the control interface ATM1/0/0.</p> <p>Enables CEF on the interface</p>
Step 3	<pre>Router(config-if)# interface XTagATM61 Router(config-if)# extended-port atm1/0/0 bpx 6.1</pre>	<p>Creates an XTagATM interface (XTagATM61).</p> <p>Associates the XTagATM interface with an external interface (BXP port 6.1) on the remotely controlled ATM switch.</p> <p>atm1/0/0 identifies the ATM interface used to control the remote ATM switch.</p>
Step 4	<pre>Router(config-if)# ip unnumbered loopback0</pre>	<p>Makes XTagATM61 an unnumbered interface and uses the IP address of loopback 0 as a substitute. The interfaces in an ATM MPLS network should usually be unnumbered. This reduces the number of IP destination-prefixes in the routing table, which reduces the number of labels and LVCs used in the network.</p>

	Command	Purpose
Step 5	Router(config-if)# mpls ip Router(config-if)# mpls atm vpi 2-5 Router(config-if)# exit	Enables MPLS on the XTagATM interface. Limits the range so that the total number of VPIs does not exceed 4. For example: mpls atm vpi 2-5 mpls atm vpi 10-13
Step 6	Router(config-if)# interface XTagATM122 Router(config-if)# extended-port atm1/0/0 bpx 12.2	Configures MPLS on another XTagATM interface and binds it to BPX port 12.2.
Step 7	Router(config-if)# ip unnumbered loopback0	Makes XTagATM122 an unnumbered interface and uses the IP address of loopback 0 as a substitute. The interfaces in an ATM MPLS network should usually be unnumbered. This reduces the number of IP destination-prefixes in the routing table, which reduces the number of labels and LVCs used in the network.
Step 8	Router(config-if)# mpls ip Router(config-if)# mpls atm vpi 2-5 Router(config-if)# exit	Enables MPLS on the XTagATM interface. Limit the range so that the total number of VPIs does not exceed 4. For example: mpls atm vpi 2-5 mpls atm vpi 10-13
Step 9	Router(config)# ip cef	Enables Cisco Express Forwarding (CEF) switching.
Step 10	Router(config)# mpls atm disable-headend-vc	Disables headend VC label advertisement.

Configuration Steps: Configuring the Cisco 6400 UAC NSP for MPLS Connectivity to the BPX Switch

To configure the Cisco 6400 UAC NSP for MPLS connectivity to the BXP switch, perform the following steps:

	Command	Purpose
Step 1	Router# show hardware 3/0 NRP 00-0000-00	Shows the hardware connected to the Cisco 6400 UAC, including the position (3/0) of the NRP in the Cisco 6400 chassis, as shown in the sample output at the left.
Step 2	Router(config)# interface atm3/0/0	Specifies the ATM interface for which you want to configure PVCs and PVPs.

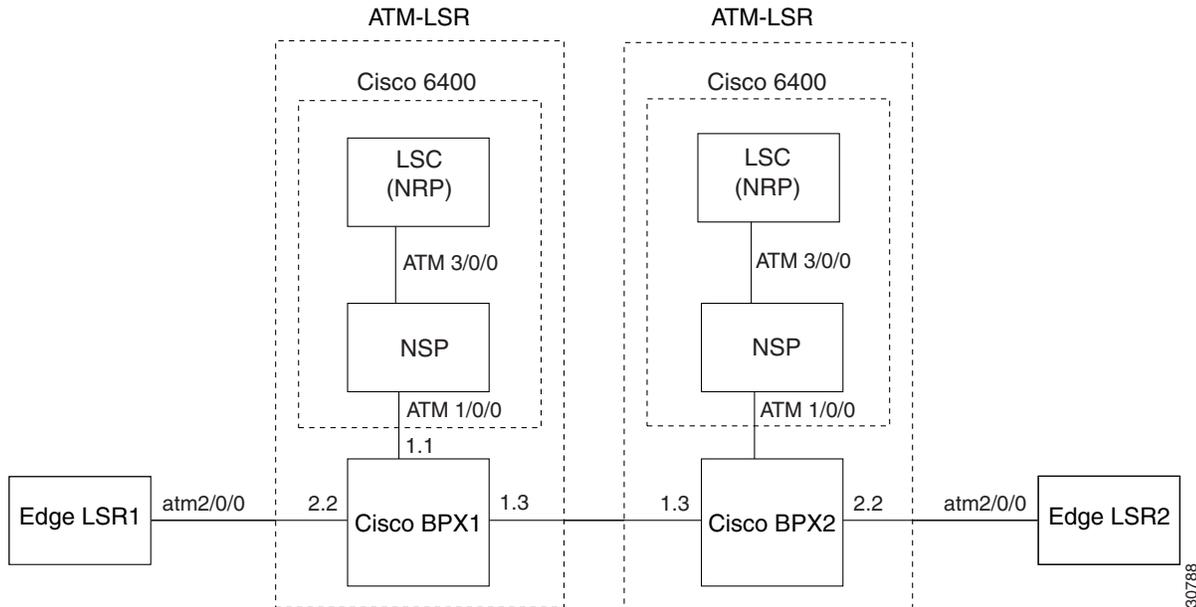
	Command	Purpose
Step 3	<pre>Switch(config-if)# atm pvc 0 40 interface ATM1/0/0 0 40 atm pvc 0 41 interface ATM1/0/0 0 41 atm pvc 0 42 interface ATM1/0/0 0 42 atm pvc 0 43 interface ATM1/0/0 0 43 atm pvc 0 44 interface ATM1/0/0 0 44 atm pvc 0 45 interface ATM1/0/0 0 45 atm pvc 0 46 interface ATM1/0/0 0 46 atm pvc 0 47 interface ATM1/0/0 0 47 atm pvc 0 48 interface ATM1/0/0 0 48 atm pvc 0 49 interface ATM1/0/0 0 49 atm pvc 0 50 interface ATM1/0/0 0 50 atm pvc 0 51 interface ATM1/0/0 0 51 atm pvc 0 52 interface ATM1/0/0 0 52 atm pvc 0 53 interface ATM1/0/0 0 53</pre>	<p>Configures the PVC for the VSI control channel¹, depending on which of the 14 slots in the Cisco BPX switch is occupied by a Cisco Broadband Switch Module (BXM). If you do not know the BPX slots containing a BXM, configure all 14 PVCs (as shown opposite) to ensure that the NSP functions properly.</p> <p>However, if you know that Cisco BPX switch slots 10 and 12, for example, contain a BXM, you only need to configure PVCs corresponding to those slots, as shown below:</p> <pre>atm pvc 0 49 interface ATM1/0/0 0 49 atm pvc 0 51 interface ATM1/0/0 0 51</pre> <p>Instead of configuring multiple PVCs, as shown opposite in this step, you can configure PVP 0 by deleting all well-known VCs. For example, you can use the command atm manual-well-known-vc delete on both interfaces and then configure PVP 0, as indicated below:</p> <pre>atm pvp 0 interface ATM1/0/0 0</pre>
Step 4	<pre>Switch(config-if)# atm pvp 2 interface ATM1/0/0 2 atm pvp 3 interface ATM1/0/0 3 atm pvp 4 interface ATM1/0/0 4 atm pvp 5 interface ATM1/0/0 5</pre>	<p>Configures the PVPs for the LVCs. For XTagATM interfaces, use the VPI range 2 through 5 (by issuing an mpls atm vpi 2-5 command). To use a different VPI range, configure the PVPs accordingly.</p>

1. Do not enable MPLS on this interface.

Configuration Example: Configuring a Cisco 6400 NRP as an LSC

When you use the NRP as an MPLS LSC in the Cisco 6400 UAC, you must configure the NSP to provide connectivity between the NRP and the Cisco BPX switch. When configured in this way (as shown in [Figure 14](#)), the NRP is connected to the NSP by means of the internal interface ATM3/0/0, while external connectivity from the Cisco 6400 UAC to the Cisco BPX switch is provided by means of the external interface ATM1/0/0 from the NSP.

Figure 14 Cisco 6400 UAC NRP Operating as an LSC



Configuration for Cisco 6400 UAC NSP

6400 NSP:

```

!
interface ATM3/0/0
  atm pvp 0 interface ATM1/0/0 0
  atm pvp 2 interface ATM1/0/0 2
  atm pvp 3 interface ATM1/0/0 3
  atm pvp 4 interface ATM1/0/0 4
  atm pvp 5 interface ATM1/0/0 5
  atm pvp 6 interface ATM1/0/0 6
  atm pvp 7 interface ATM1/0/0 7
  atm pvp 8 interface ATM1/0/0 8
  atm pvp 9 interface ATM1/0/0 9
  atm pvp 10 interface ATM1/0/0 10
  atm pvp 11 interface ATM1/0/0 11
  atm pvp 12 interface ATM1/0/0 12
  atm pvp 13 interface ATM1/0/0 13
  atm pvp 14 interface ATM1/0/0 14
  atm pvp 15 interface ATM1/0/0 15

```



Note

Instead of configuring multiple PVCs, you can also configure PVP 0 by deleting all well-known VCs. For example, you can use the command **atm manual-well-known-vc delete** on both interfaces and then configure PVP 0, as indicated below:

```
atm pvp 0 interface ATM1/0/0 0
```

Configuration for Cisco 6400 UAC NRP LSC1

```

ip cef
!
interface Loopback0
  ip address 172.18.143.22 255.255.255.255
!

```

```

interface ATM0/0/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
  ip unnumbered Loopback0
  extended-port ATM0/0/0 bpx 1.3
  mpls atm vpi 2-15
  mpls ip
!
interface XTagATM22
  ip unnumbered Loopback0
  extended-port ATM0/0/0 bpx 2.2
  mpls atm vpi 2-5
  mpls ip
!
mpls atm disable-headend-vc

```

Configuration for BPX1 and BPX2

BPX1 and BPX2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3
cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```



Note

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for instance, XTagATM11).

Configuration for Cisco 6400 UAC NRP LSC2

```

ip cef
!
interface Loopback0
  ip address 172.103.210.5 255.255.255.255
!
interface ATM0/0/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
  ip unnumbered Loopback0
  extended-port ATM0/0/0 bpx 1.3
  mpls atm vpi 2-15
  mpls ip
!
interface XTagATM22
  ip unnumbered Loopback0
  extended-port ATM0/0/0 bpx 2.2
  mpls atm vpi 2-5
  mpls ip
!
mpls atm disable-headend-vc

```

Configuration for Edge LSR1

LSR1:

```
ip cef distributed
!
interface loopback 0
  ip address 172.22.132.2 255.255.255.255
!
interface ATM2/0/0
  no ip address
!
interface ATM2/0/0.22 mpls
  ip unnumbered loopback 0
  mpls atm vpi 2-5
  mpls ip
```

Configuration for Edge LSR2

LSR2:

```
ip cef distributed
!
interface loopback 0
  ip address 172.22.172.18 255.255.255.255
!
interface ATM2/0/0
  no ip address
!
interface ATM2/0/0.22 mpls
  unnumbered loopback 0
  mpls atm vpi 2-5
  mpls ip
```

Configuring the Cisco IGX 8400 Switch with a Universal Router Module as an MPLS ATM-LSR

Cisco offers the Universal Router Module (URM) for the Cisco IGX 8400 series switches. The Universal Router Module is a blade for the IGX switch. The IGX switch with the URM supports MPLS and can function as an MPLS ATM-LSR. The following sections explain how to configure the IGX switch with the URM as an MPLS ATM-LSR.

Running the URM on the IGX requires Switch Software 9.3.20 or higher.

VSI

The Virtual Switch Interface (VSI) allows MPLS controllers to control the switch. Each URM in an IGX can be a VSI master or slave. The embedded router in the URM can be configured as a router. The embedded universal switching module (UXM) is always a VSI slave. The embedded router on the URM can act as a master to communicate with the slaves on the IGX and control switch resources.

ATM-LSR

The URM supports MPLS, enabling it to function as an ATM-LSR. The interfaces have the following functions:

- LC-ATM-based ATM interfaces support the ATM-LSR.
- ATM Edge LSR interfaces support MPLS imposition and disposition.

**Note**

The URM cannot act as both an Edge LSR and ATM-LSR. You can disable the URM from acting as an Edge LSR with the **mpls atm disable-headend-vc** command. By default, the Edge LSR functionality is enabled.

Cisco IGX 8400 Switch with a Universal Router Module Overview

The URM consists of a logically partitioned front card connected to a universal router interface (URI) back card. The front card contains an embedded UXM-E running an Administration firmware image, and an embedded router (based on the Cisco 3660 router) running a Cisco IOS image. The embedded UXM-E and the embedded router connect through a logical internal ATM interface, with capability equivalent to an OC-3 ATM port.

**Note**

SWSW treats this interface as an OC-3 ATM port, and this interface is the only port on the embedded UXM-E that is visible to SWSW.

Unlike the Cisco 3660 router, which has one slot for the motherboard and six slots for network modules, the embedded router has three virtual slots with built-in interfaces (see [Table 6](#)).

Table 6 *Interfaces Found on Embedded Router Virtual Slots*

Slot	Name	Description
Slot 0	ATM 0/0	The internal ATM interface connected to the embedded UXM-E ATM port.
Slot 1	FE1/0 and FE1/1	Fast Ethernet interfaces connected to the Fast Ethernet ports on the BC-URI-2FE2V back card.
Slot 2	T1 2/0 and T1 2/1; E1 2/0 and E1 2/1	T1 or E1 interfaces connected to the T1 or E1 ports on the VWIC installed in the back card.

Because the URM front card contains both an embedded UXM-E and an embedded Cisco router, the front card runs two separate software images with two different download procedures. For the embedded UXM-E, the Administration firmware image (Version XAA) is downloaded and saved to the embedded UXM-E Flash memory through SWSW command-line interface (CLI) commands, which are documented in [Cisco IGX 8400 Series Installation and Configuration](#).

The embedded router runs Cisco IOS software. You can download and save the Cisco IOS image using standard Cisco IOS procedures as outlined in any documentation supporting Cisco IOS Release 12.1(5)YA or later (see the [Cisco IOS Configuration Fundamentals Configuration Guide](#)).

The embedded UXM-E hardware is based on the UXM-E card for the Cisco IGX series and features 16-MB asynchronous DRAM, 8-MB Flash memory, and 8-KB BRAM. The embedded router hardware is based on the Cisco 3660 modular-access router and features 8-MB boot Flash SIMM, 32-MB Cisco IOS Flash SIMM, and 128-KB NVRAM.

The back card (BC-URI-2FE2VT1 or BC-URI-2FE2VE1) contains an installed voice and WAN interface card (VWIC) with a generic dual-port T1 or E1 digital voice interface.

URM Connections

The Cisco IGX backplane is a cell bus composed of four parallel data buses that transmit up to four cells at a time. This bus bandwidth is organized into allocated units called universal bandwidth units (UBUs), each capable of transmitting 4000 cells per second or 2000 fast packets per second. The Cisco IGX has a total of 584 UBUs, giving the Cisco IGX the capacity to transmit about 2 million cells or 1 million fast packets per second.

Each URM receives a default bandwidth from the Cisco IGX at power on. You can configure this default bandwidth by using the SWSW CLI `cnfbusbw` command. For more information on this and other SWSW commands, refer to the [Cisco WAN Switching Command Reference](#).



Note

Except for slots 1 and 2 (which are reserved for the NPM), all slots in the Cisco IGX can be used to support a URM. However, the total number of UBUs allocated to all cards supported in the Cisco IGX cannot exceed the total Cisco IGX backplane bandwidth.

Connections terminating on the URM can be virtual path connections (VPCs) or virtual channel connections (VCCs).

The Cisco IOS router in the URM connects to Cisco IGX WAN through an internal ATM interface on the URM card. Because the URM supports voice connections using either standard VoIP or Cisco proprietary VoATM configurations (using ATM PVCs on the internal ATM interface), the remote end of these connections is either an ATM PVC endpoint or a Frame Relay PVC endpoint.



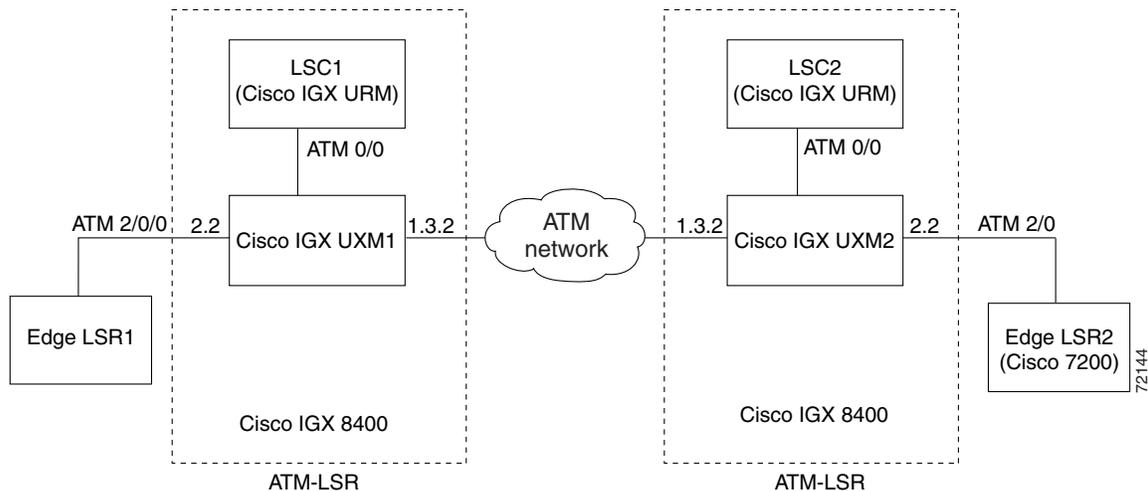
Note

For more information about the URM for Cisco IGX 8400, see the [Update to Cisco IGX 8400 Series Installation and Configuration and Reference](#).

Configuration Example: Configuring a Cisco IGX 8400 Switch with a URM as an MPLS ATM-LSR

The following example configures MPLS on ATM-LSRs and Edge LSRs. The examples use the appropriate ATM interfaces that are directly connected to IGX.

Figure 15 Cisco IGX 8400 Switch with a Universal Router Module



Configuration for Edge LSR 1

LSR1:

```

ip cef distributed
interface loopback 0
    ip address 172.22.132.2 255.255.255.255
    !
interface ATM2/0/0
    no ip address
    !
interface ATM2/0/0.22 mpls
    ip unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip

```

Configuration for ATM-LSR1

URM LSC1:

```

ip cef
mpls atm disable-headend-vc
!
interface loopback0
    ip address 2.2.2.2 255.255.255.0
!
interface atm0/0
no shut
tag-control-protocol vsi id 1
ip route-cache cef
!
interface XTagATM132
    extended-port atm0/0 igx 1.3.2
    ip unnumbered loopback0
    mpls atm vp-tunnel 2
    mpls ip
!
interface XTagATM22
    extended-port atm0/0 igx 2.2
    ip unnumbered loopback0
    mpls atm vpi 2-5
    mpls ip

```

Configuration for ATM-LSR2

URM LSC2

```

ip cef
mpls atm disable-headend-vc
interface loopback0
    ip address 3.3.3.3 255.255.255.255
!
interface atm0/0
no shut
tag-control-protocol vsi id 2
ip route-cache cef
!
interface XTagATM132
    ip unnumbered loopback0
    extended-port atm0/0 igx 1.3.2
    mpls atm vp-tunnel 2
    mpls ip

```

```

interface XTagATM22
  ip unnumbered loopback0
  extended-port atm0/0 igx 2.2
  mpls atm vpi 2-5
  mpls ip

```

Configuration for IGX1 and IGX2

IGX1 and IGX2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3.2
cnftrk 1.3.2 100000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,RT-VBR N TERRESTRIAL 10
0 N N Y Y Y CBR 2
cnfrsrc 1.3.2 256 252207 y 1 e 512 6144 2 2 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```



Note

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for instance, XTagATM11).

Configuration for Edge LSR2

7200 LSR2:

```

ip cef
interface loopback 0
  ip address 172.22.172.18 255.255.255.255
!
interface ATM2/0
  no ip address
!
interface ATM2/0.22 mpls
  ip unnumbered loopback 0
mpls atm vpi 2-5
mpls ip

```

Disabling the LSC from Acting as an Edge LSR

Using the MPLS LSC as a label edge device is *not* supported. Using the MPLS LSC as a label edge device introduces unnecessary complexity to the configuration. See the command **mpls atm disable-headend-vc** to disable edge LSR functionality on the LSC.

Disabling the LSC from acting as an edge LSR causes the LSC to stop initiating LSPs to any destination. Therefore, the number of LVCs used in the network is reduced. The LSC can still terminate tailend LVCs, if required.

You can prevent the terminating tailend LVCs from being created between the edge LSRs and LSCs. This helps prevent the unnecessary use of LVC resources in a slave ATM switch. You use the **mpls request-labels for** command with an access list to disable the creation of the LSPs. You can create an access list at an edge LSR to restrict the destinations for which a downstream-on-demand request is issued.

With downstream on demand, LVCs are depleted with the addition of each new node. These commands save resources by disabling the LSC from setting up unwanted LSPs. The absence of those LSPs allows traffic to follow the same path as control traffic.

The following example uses the **mpls atm disable-headend-vc** command to disable the LSC from functioning as an edge LSR. The following line is added to the LSC configuration:

```
mpls atm disable-headend-vc
```

**Note**

For a Cisco 6400 UAC with an NRP configured to function as an LSC, disable the LSC from acting as an edge LSR. An NRP LSC should only support label switch paths through the controlled ATM switch under VSI control.

Feature 1: Creating Virtual Trunks

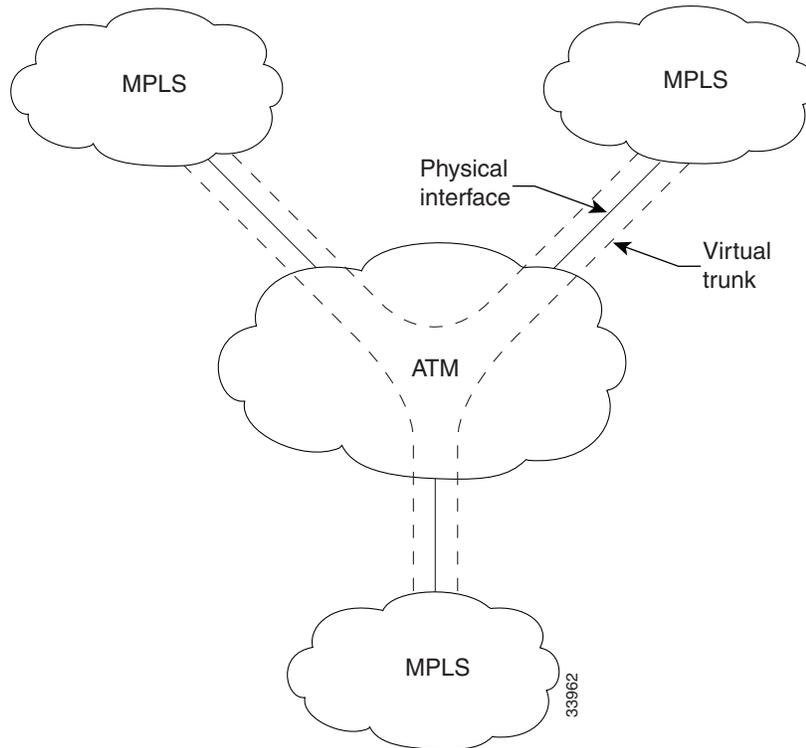
Virtual trunks provide connectivity for Cisco WAN MPLS switches through an ATM cloud, as shown in [Figure 16](#). Because several virtual trunks can be configured across a given private/public physical trunk, virtual trunks provide a cost-effective means of connecting across an entire ATM network.

The ATM equipment in the cloud must support virtual path switching and transmission of ATM cells based solely on the VPI in the ATM cell header. The virtual path identifier (VPI) is provided by the ATM cloud administrator (that is, by the service provider).

Typical ATM Hybrid Network with Virtual Trunks

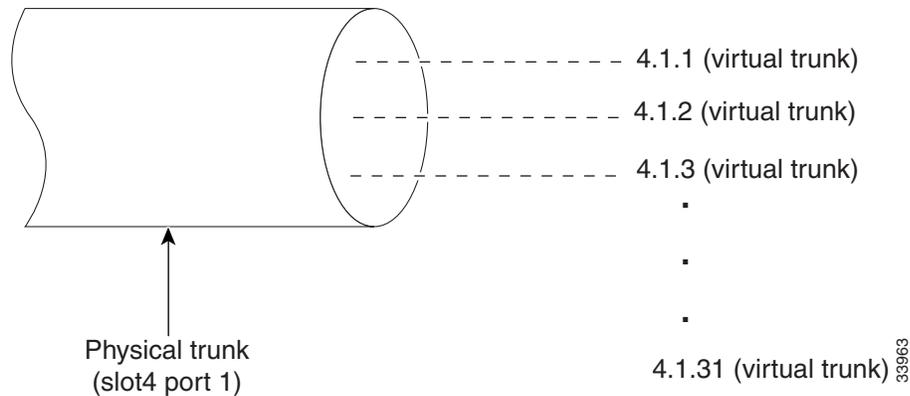
[Figure 16](#) shows three Cisco WAN MPLS switching networks, each connected to an ATM network by a physical line. The ATM network links all three of these subnetworks to every other subnetwork with a fully meshed network of virtual trunks. In this example, each physical interface is configured with two virtual trunks.

Figure 16 Typical ATM Hybrid Network Using Virtual Trunks



A virtual trunk number (slot number.port number.trunk number) differentiates the virtual trunks found within a physical trunk port. In Figure 17, three virtual trunks (4.1.1, 4.1.2, and 4.1.3) are configured on a physical trunk that connects to the port 4.1 interface of a BXM.

Figure 17 Virtual Trunks Configured on a Physical Trunk



These virtual trunks are mapped to the XTagATM interfaces on the LSC. On the XTagATM interface, you configure the respective VPI value using the command `mpls atm vp-tunnel vpi`. This VPI should match the VPI in the ATM network. The label virtual circuits (LVCs) are generated inside this VP, and this VP carries the LVCs and their traffic across the network.

Virtual Trunking Benefits

Virtual trunks provide the following benefits:

- **Reduced costs**—By sharing the resources of a single physical trunk among a number of virtual (logical) trunks, each virtual trunk provided by the public carrier needs to be assigned only as much bandwidth as needed for that interface, rather than the full T3, E3, OC-3, or OC-12 bandwidth of an entire physical trunk.
- **Migration of MPLS services into existing networks**—VSI virtual trunks allow MPLS services to be carried over part of a network that does not support MPLS services. The part of the network that does not support such services may be a public ATM network, for example, that consists of switches that are not MPLS-enabled.

Virtual Trunking Restrictions

Virtual Trunk Bandwidth—The total bandwidth of all the virtual trunks on one port cannot exceed the maximum bandwidth of the port. Trunk loading (units of load) is maintained per virtual trunk, but the cumulative loading of all virtual trunks on a port is restricted by the transmit and receive rates for the port.

Maximum Virtual Trunks—The maximum number of virtual trunks that can be configured per card equals the number of virtual interfaces (VIs) on the BPX/IGX switch.

- The BXM supports 32 virtual interfaces; hence, it supports up to 32 virtual trunks. Accordingly, you can have interfaces ranging from XTagATM411 to XTagATM4131 on the same physical interface.
- The UXM supports 16 virtual interfaces. You can have interfaces ranging from XTagATM411 to XTagATM 4116.

Configuration Example: Configuring Virtual Trunks with Cisco 7200 LSCs

The network topology shown in [Figure 18](#) incorporates two ATM-LSRs using virtual trunking to create an MPLS network through a private ATM Network. This topology includes:

- Two LSCs (Cisco 7200 routers)
- Two BPX switches
- Two Edge LSRs (Cisco 7200 routers)

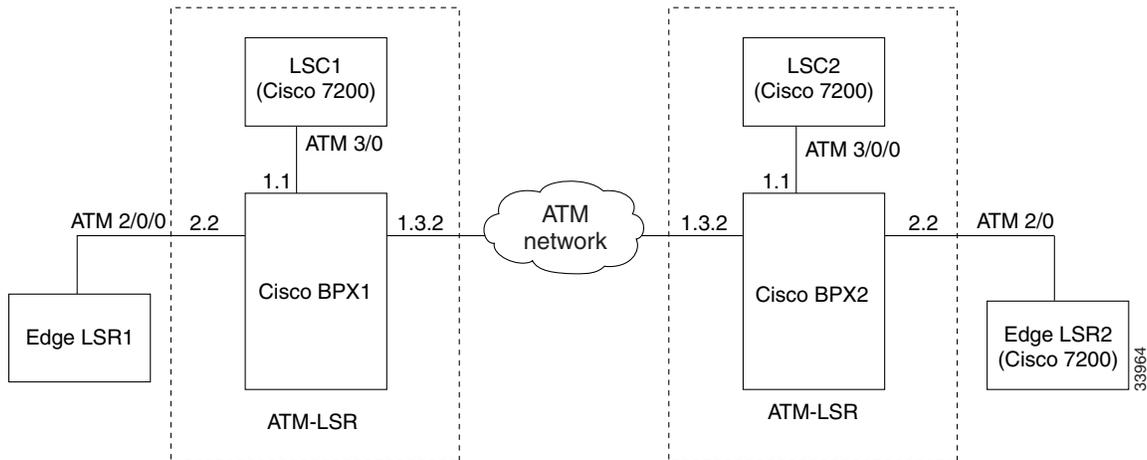


Note

For the Cisco IGX switch, use the following commands:

```
extended-port atm1/0 descriptor 0.x.x.0
tag-control-protocol vsi slaves 32 id x
ip route-cache cef
```

Figure 18 ATM-LSR Virtual Trunking through ATM Network



Based on [Figure 19](#), the following configuration examples are provided:

- [Configuration for LSC1 Implementing Virtual Trunking, page 67](#)
- [Configuration for BPX1 and BPX2, page 67](#)
- [Configuration for LSC2 Implementing Virtual Trunking, page 68](#)
- [Configuration for Edge LSR1, page 68](#)
- [Configuration for Edge LSR2, page 69](#)

Configuration for LSC1 Implementing Virtual Trunking

7200 LSC1:

```

ip cef
!
interface loopback0
 ip address 172.103.210.5 255.255.255.255
!
interface ATM3/0
 no ip address
 tag-control-protocol vsi
 ip route-cache cef
!
interface XTagATM132
 extended-port ATM3/0 bpx 1.3.2
 ip unnumbered loopback0
 mpls atm vp-tunnel 2
 mpls ip
!
interface XTagATM22
 extended-port ATM3/0 bpx 2.2
 ip unnumbered loopback0
 mpls atm vpi 2-5
 mpls ip

```

Configuration for BPX1 and BPX2

BPX1 and BPX2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3.2
cnftrk 1.3.2 100000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,RT-VBR N TERRESTRIAL 10
0 N N Y Y Y CBR 2
cnfrsrc 1.3.2 256 252207 y 1 e 512 6144 2 2 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```

**Note**

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for instance, XTagATM11).

Configuration for LSC2 Implementing Virtual Trunking

7200 LSC2:

```

ip cef
!
interface loopback0
    ip address 172.18.143.22 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM132
    extended-port ATM3/0 bpx 1.3.2
    ip unnumbered loopback0
    mpls atm vp-tunnel 2
    mpls ip
!
interface XTagATM22
    extended-port ATM3/0 bpx 2.2
    ip unnumbered loopback0
    mpls atm vpi 2-5
    mpls ip

```

Configuration for Edge LSR1

LSR1:

```

ip cef distributed
interface loopback 0
    ip address 172.22.132.2 255.255.255.255
!
interface ATM2/0/0
    no ip address
!
interface ATM2/0/0.22 mpls
    ip unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip

```

Configuration for Edge LSR2

7200 LSR2:

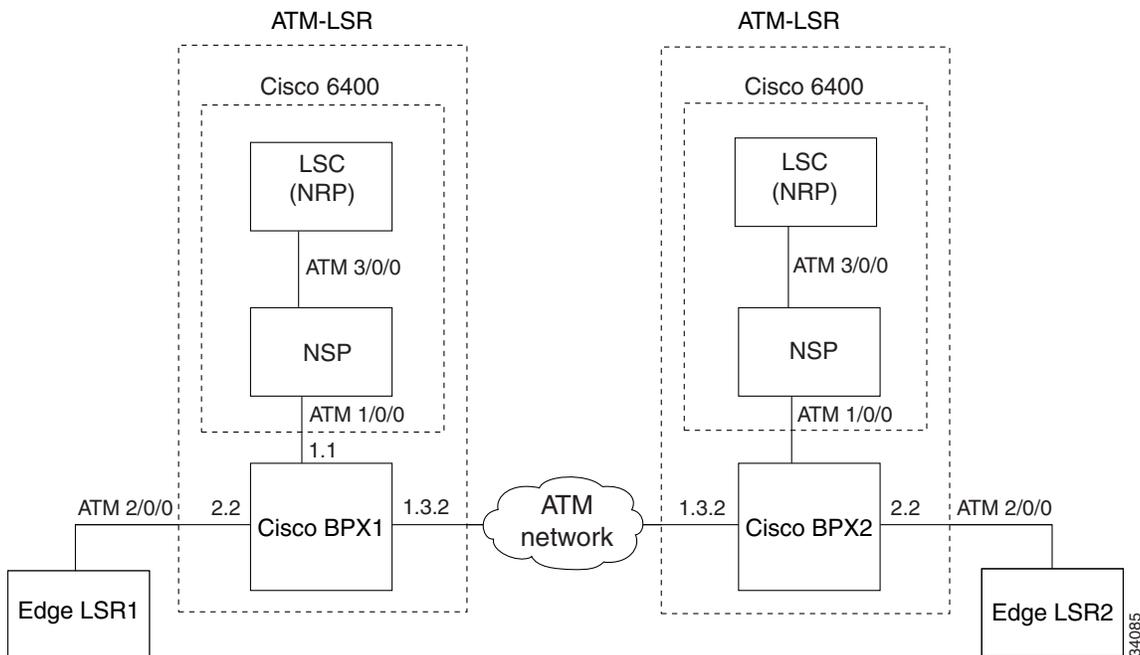
```
ip cef
interface loopback 0
  ip address 172.22.172.18 255.255.255.255
!
interface ATM2/0
  no ip address
!
interface ATM2/0.22 mpls
  ip unnumbered loopback 0
  mpls atm vpi 2-5
  mpls ip
```

Configuration Example: Configuring Virtual Trunking on Cisco 6400 NRP LSCs

The network topology shown in [Figure 19](#) incorporates two ATM-LSRs using virtual trunking to create an MPLS network through a private ATM Network. This topology includes:

- Two LSCs (Cisco 6400 UAC NRP routers)
- Two BPX switches
- Two Edge LSRs (Cisco 7200 routers)

Figure 19 Cisco 6400 NRP Operating as LSC Implementing Virtual Trunking



Configuration for Cisco 6400 UAC NSP

6400 NSP:

```
!
```

```

interface ATM3/0/0
  atm pvp 0 interface ATM1/0/0 0
  atm pvp 2 interface ATM1/0/0 2
  atm pvp 3 interface ATM1/0/0 3
  atm pvp 4 interface ATM1/0/0 4
  atm pvp 5 interface ATM1/0/0 5
  atm pvp 6 interface ATM1/0/0 6
  atm pvp 7 interface ATM1/0/0 7
  atm pvp 8 interface ATM1/0/0 8
  atm pvp 9 interface ATM1/0/0 9
  atm pvp 10 interface ATM1/0/0 10
  atm pvp 11 interface ATM1/0/0 11
  atm pvp 12 interface ATM1/0/0 12
  atm pvp 13 interface ATM1/0/0 13
  atm pvp 14 interface ATM1/0/0 14
  atm pvp 15 interface ATM1/0/0 15

```

**Note**

Instead of configuring multiple PVCs, you can also configure PVP 0 by deleting all well-known VCs. For example, you can use the **atm manual-well-known-vc delete** command on both interfaces and then configure PVP 0, as indicated below:

atm pvp 0 interface ATM1/0/0 0

Configuration for Cisco 6400 UAC NRP LSC1 Implementing Virtual Trunking

```

ip cef
!
interface Loopback0
  ip address 172.18.143.22 255.255.255.255
!
interface ATM0/0/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM132
  ip unnumbered Loopback0
  extended-port ATM0/0/0 bpx 1.3.2
  mpls atm vp-tunnel 2
  mpls ip
!
interface XTagATM22
  ip unnumbered Loopback0
  extended-port ATM0/0/0 bpx 2.2
  mpls atm vpi 2-5
  mpls ip
!
mpls atm disable-headend-vc

```

Configuration for BPX1 and BPX2

BPX1 and BPX2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3.2
cnftrk 1.3.2 100000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,RT-VBR N TERRESTRIAL 10
0 N N Y Y Y CBR 2

```

```

cnfrsrc 1.3.2 256 252207 y 1 e 512 6144 2 2 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```

**Note**

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for instance, XTagATM11).

Configuration for 6400 UAC NRP LSC2 Implementing Virtual Trunking

```

ip cef
!
interface Loopback0
    ip address 172.103.210.5 255.255.255.255
!
!
interface ATM0/0/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM132
    ip unnumbered Loopback0
    extended-port ATM0/0/0 bpx 1.3.2
    mpls atm vp-tunnel 2
    mpls ip
!
interface XTagATM22
    ip unnumbered Loopback0
    extended-port ATM0/0/0 bpx 2.2
    mpls atm vpi 2-5
    mpls ip
!
mpls atm disable-headend-vc

```

Configuration for Edge LSR1

LSR1:

```

ip cef distributed
!
interface loopback 0
    ip address 172.22.132.2 255.255.255.255
!
interface ATM2/0/0
no ip address
!
interface ATM2/0/0.22 mpls
    ip unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip

```

Configuration for Edge LSR2

LSR2:

```

ip cef distributed
!
interface loopback 0

```

```
        ip address 172.22.172.18 255.255.255.255
    !
interface ATM2/0/0
    no ip address
    !
interface ATM2/0/0.22 mpls
    unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip
```

Feature 2: Using LSC Redundancy

LSC redundancy allows you to create a highly reliable IP network, one whose reliability is nearly equivalent to that provided by hot standby routing. Instead of using hot standby routing processes to create redundancy, this method uses a combination of LSCs, the Virtual Switch Interface (VSI), and IP routing paths with the same cost path for hot redundancy, or different costs for warm redundancy. The VSI allows multiple control planes (MPLS, PNNI, and voice) to control the same switch. Each control plane controls a different partition of the switch.

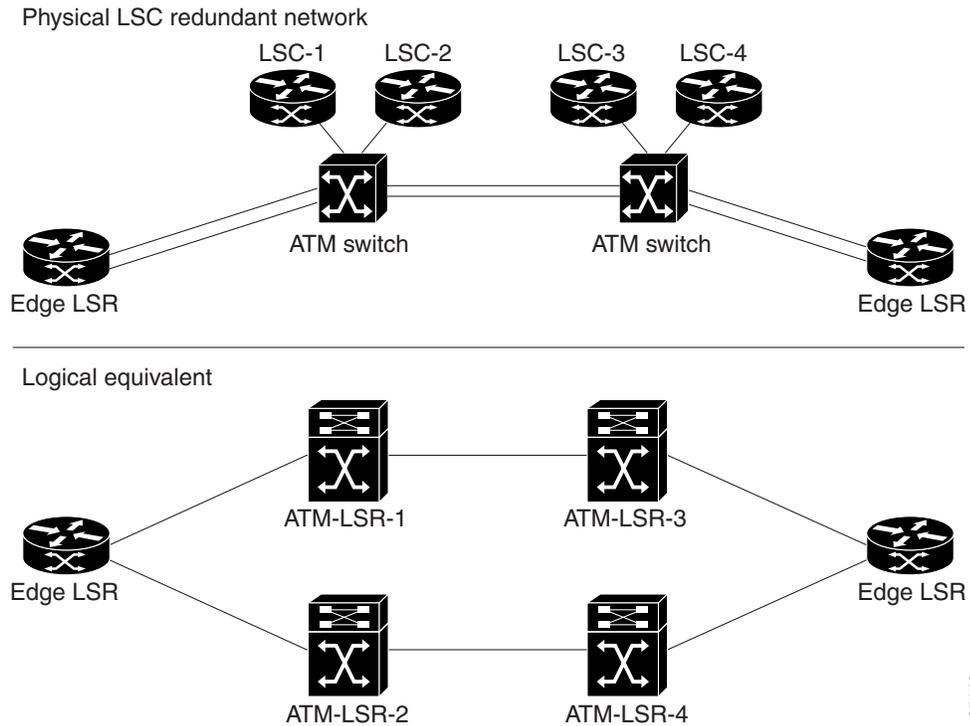
In the LSC redundancy model, two independent LSCs control the different partitions of the switch. Thus, two separate MPLS control planes set up connections on different partitions of the same switch. This is where LSC redundancy differs from hot standby redundancy. The LSCs do not need copies of each other's internal state to create redundancy. The LSCs control the partitions of the switch independently.

A single IP network consists of switches with one LSC (or a hot standby pair of LSCs) and MPLS edge label switch routers (LSRs).

If you change that network configuration by assigning two LSCs per switch, you form two separate MPLS control planes for the network. You logically create two independent parallel IP subnetworks linked at the edge.

If the two LSCs on each switch are assigned identical shares of the switch's resources and links, the two subnetworks are identical. You have two identical parallel IP subnetworks on virtually the same equipment, which would otherwise support only one network.

For example, [Figure 20](#) shows a network of switches that each have two LSCs. MPLS Edge LSRs are located at the edge of the network, to form a single IP network. The LSCs on each switch have identical shares of the switch's resources and links, which makes the networks identical. In other words, there are two identical parallel IP subnetworks.

Figure 20 LSC Redundancy Model

Part of the redundancy model includes Edge LSRs, which link the two networks at the edge.

If the network uses Open Shortest Path First (OSPF) or a similar IP routing protocol with an equal cost on each path, then there are at least two equally viable paths from every Edge LSR to every other Edge LSR. The OSPF equal cost multipath distributes traffic evenly on both paths. Therefore, MPLS sets up two identical sets of connections for the two MPLS control planes. IP traffic travels equally across the two sets of connections.

**Note**

The LSC redundancy model works with any routing protocol. For example, you can use Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS). Also, you can use both the Tag Distribution Protocol (TDP) and the Label Distribution Protocol (LDP).

With the LSC redundancy model, if one LSC on a switch fails, IP traffic uses the other path, without having to establish new links. LSC redundancy does not require the network to set up new connections when a controller fails. Because the connections to the other paths have already been established, the interruption to the traffic flow is negligible. The LSC redundancy model is as reliable as networks that use hot standby controllers. LSC redundancy requires hardware like that used by hot standby controllers. However, the controllers act independently, rather than in hot standby mode. For LSC redundancy to work, the hardware must have connection capacity for doubled-up connections.

If an LSC fails and LSC redundancy is not present, IP traffic halts until other switches break their present connections and reroute traffic around the failed controller. The stopped IP traffic results in undesirable unreliability.

Hot LSC Redundancy

Hot redundancy provides near-instant failover to the other path when an LSC fails. When you set up hot redundancy, both LSCs are active and have the same routing costs on both paths. To ensure that the routing costs are the same, run the same routing protocols on the redundant LSCs.

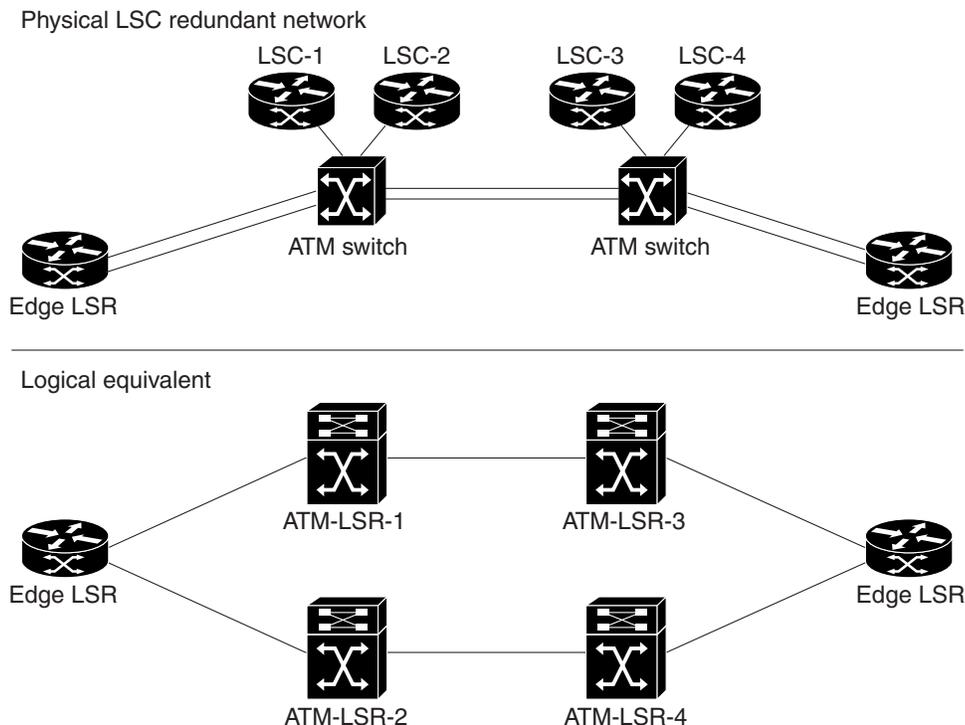
In hot redundancy, the LSCs run parallel and independent Label Distribution Protocols (LDPs). At the Edge LSRs, when the LDP has multiple routes for the same destination, it requests multiple labels. It also requests multiple labels when it needs to support class of service (CoS). When one LSC fails, the labels distributed by that LSC are removed.

To achieve hot redundancy, you can implement the following redundant components:

- Redundant physical interfaces between the Edge LSR and the ATM-LSR to ensure reliability in case one physical interface fails.
- Redundant interfaces or redundant VP tunnels between the ATM switches.
- Slave ATM switches, such as the BPX 8650, can have redundant control cards and switch fabrics. If redundant switch fabrics are used and the primary switch fails, the other switch fabric takes over.
- Redundant LSCs.
- The same routing protocol running on both LSCs. (You can have different tag/label distribution protocols.)

Figure 21 shows one example of how hot LSC redundancy can be implemented.

Figure 21 Hot LSC Redundancy



35149

Warm LSC Redundancy

To achieve warm redundancy, you need only redundant LSCs. You do not necessarily need to run the same routing protocols or distribution protocols on the LSCs.

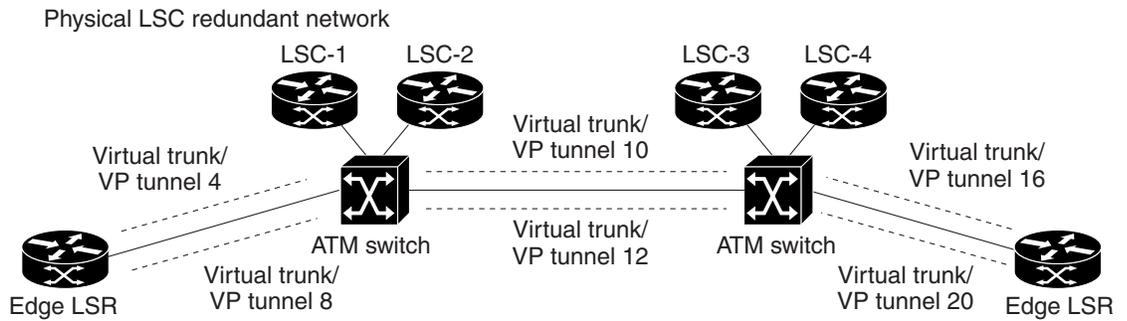
Note

You can use different routing protocols on parallel LSCs. However, you do not get near-instant failover. The failover time includes the time it takes to reroute the traffic, plus the LDP bind request time. If the primary routing protocol fails, the secondary routing protocol finds new routes and creates new label virtual circuits (LVCs). An advantage to using different routing protocols is that the ATM switch uses fewer resources and offers more robust redundancy.

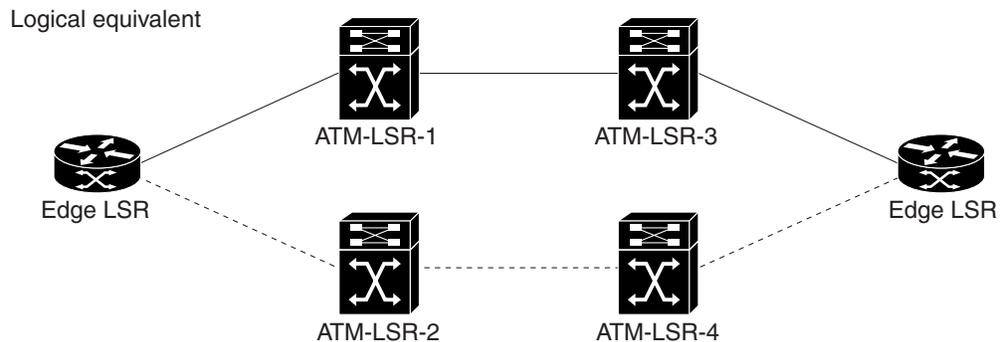
If you run the same routing protocols, you specify a higher cost for the interfaces on the backup LSC. This causes the data to use only the lower-cost path. This also saves resources on the ATM switch, because the Edge LSR requests LVCs only through the lower-cost LSC. When the primary LSC fails, the Edge LSR uses the backup LSC and creates new paths to the destination. Creating new paths requires reroute time and LDP negotiation time.

Figure 22 shows one example of how warm LSC redundancy can be implemented.

Figure 22 Warm LSC Redundancy



Note: Tunnels are virtual interfaces. -----
 Physical interfaces are marked by thin lines. _____



35152

Differences Between Hot and Warm LSC Redundancy

Virtually any configuration of switches and LSCs that provides hot redundancy can also provide warm redundancy. You can also switch from warm to hot redundancy with little or no change to the links, switch configurations, or partitions.

Hot and warm redundancy differ in the following ways:

- Hot redundancy uses both paths to route traffic. You set up both paths using equal cost multipath routing, so that traffic is load balanced between the two paths. As a result, hot redundancy uses twice the number of MPLS label VCs as warm redundancy.
- Warm redundancy uses only one path at a time. You set up the paths so that one path has a higher cost than the other. Traffic only uses one path and the other path is a backup path.

General Redundancy Operational Modes

The LSC redundancy model allows you to use the following four operational models. Most other redundancy models cannot accommodate all of these redundancy models.

- **Transparent Mode**—The primary and secondary redundant systems have the same copies of the image and startup configurations. When one system fails, the other takes over, and the operations are identical. However, this mode risks software failures, because both systems use the same algorithms. A software problem on the primary system is likely to affect the secondary system as well.
- **Upgrade mode**—You can upgrade the image or configuration of the redundant system, without rebooting the entire system. You can use this mode to change the resources between different partitions of the slave ATM switch.
- **Nontransparent mode**—The primary and secondary systems have different images or configurations. This mode is more reliable than transparent mode, which loads the same software on both controllers. In nontransparent mode, the use of different images and configurations reduces the risk of both systems encountering the same problem.
- **Experimental mode**—You load an experimental version of the image or configuration on the secondary system. You can use experimental mode when you want to test the new images in a real environment.

How LSC Redundancy Differs from Router and Switch Redundancy

In traditional IP router networks, network managers ensure reliability by creating multiple paths through the network from every source to every destination. If a device or link on one path fails, IP traffic uses an alternate path to reach its destination.

LSC Redundancy

Connecting two independent LSCs to each switch by the Virtual Switch Interface (VSI) creates two identical subnetworks. Multipath IP routing uses both subnetworks equally. Thus, both subnetworks have identical connections. If a controller in one subnetwork fails, the multipath IP routing diverts traffic to the other path. Because the connections already exist in the alternate path, the reroute time is very fast. The LSC redundancy model matches the reliability of networks with hot standby controllers, without the difficulty of implementing hot standby redundancy.

Router Redundancy

Because routers do not need to establish a virtual circuit to transfer data, they are inherently connectionless. When a router discovers a failed device or link, it requires approximately less than a second to reroute traffic from one path to another.

Routers can incorporate a warm or hot standby routing process to increase reliability. The routing processes share information about the routes to direct different streams of IP traffic. They do not need to keep or share connection information. Routers can also include redundant switch fabrics, backplanes, power supplies, and other components to decrease the chances of node failures.

ATM, Frame Relay, and Circuit Switch Redundancy

Circuit switch, ATM, and Frame Relay networks transfer data by establishing circuits or virtual circuits. To ensure the transfer of data in switches, network managers incorporate redundant switch components. If any component fails, a spare component takes over. Switches can have redundant line cards, power supplies, fans, backplanes, switch fabrics, line cards, and control cards.

- The redundant backplanes include all the hardware to operate two backplanes and to switch to the backup backplane if one fails.
- Redundant line cards protect against failed links. If a link to a line card fails, the redundant line card takes over. To create redundant line cards, you must program the same connection information into both line cards. This ensures that the circuits or virtual circuits are not disrupted when the new line card takes over.
- The redundant switch fabric must also have the same connection information as the active switch fabric.

A software application usually monitors the state of the switches and their components. If a problem arises, the software sets an alarm to bring attention to the faulty component.

The redundant switch hardware and software are required, because switches take some time to reroute traffic when a failure occurs. Switches can have connection routing software, such as Cisco automatic connection routing, PNNI, or MPLS. However, rerouting the connections in a switch takes much more time than rerouting traffic in a router network. Rerouting connections in a switch requires calculating routes and reprogramming some hardware for each connection. In router networks, large aggregates of traffic can be rerouted simultaneously, with little or no hardware programming. Therefore, router networks can reroute traffic more quickly and easily than connection-oriented networks. Router networks rely on rerouting techniques to ensure reliability. Connection-oriented networks use rerouting only as a last resort.

General Hot/Warm Standby Redundancy in Switches

Network managers can install redundant copies of the connection routing software for ATM and Frame Relay switches on a redundant pair of control processors.

With hot standby redundancy, the active process sends its state to the spare process to keep the spare process up to date in case it needs to take over. The active process sends the state information to the spare process or writes the state to a disk, where both processes can access the information. In either case, the state information is shared between controllers. Because the state of the network routing tables changes frequently, the software must perform much work to maintain consistent routing states between redundant pairs of controllers.

With warm standby redundancy, the state information is not shared between the active and spare processes. If a failure occurs, the spare process resets all of the connections and re-establishes them. Reliability decreases when the spare resets the connections. The chance of losing data increases.

LSC Redundancy Benefits

By implementing the LSC redundancy model, you eliminate the single point of failure between the LSC and the ATM switch it controls. If one LSC fails, the other LSC takes over and routes the data on the other path. The following sections explain the other benefits of LSC redundancy.

LSC Redundancy Does Not Use Shared States or Databases

In the LSC redundancy model, the LSCs do not share states or databases, which increases reliability. Sometimes, when states and databases are shared, an error in the state or database information can cause both controllers to fail simultaneously.

Also, new software features and enhancements do not affect LSC redundancy. Because the LSCs do not share states or database information, you do not have to worry about ensuring redundancy during every step of the update.

LSC Redundancy Allows Different Software Versions

The LSCs work independently and there is no interaction between the controllers. They do not share the controller's state or database, as other redundancy models require. Therefore, you can run different versions of the IOS software on the LSCs, which provides the following advantages:

- You can test the features of the latest version of software without risking reliability. You can run the latest version of the IOS software on one LSC and an older version of the IOS software on a different LSC. If the LSC running the new IOS software fails, the LSC running the older software takes over.
- Running different versions of the IOS software reduces the chance of having both controllers fail. If you run the same version of the IOS software on both controllers and that version contains a problem, it could cause both controllers to fail. Running different versions on the controllers eliminates the possibility of each controller failing because of the same problem.



Note

Using different IOS software version on different LSCs is recommended only as a temporary measure. Different versions of IOS software in a network could be incompatible, although it is unlikely. For best results, run the same version of IOS software on all devices.

LSC Redundancy Allows You to Use Different Router Models

You can use different models of routers in this LSC redundancy model. Using different hardware in the redundancy model reduces the chance that a hardware fault would interrupt network traffic.

LSC Redundancy Allows You to Switch from Hot to Warm Redundancy on the Fly

You can implement hot or warm redundancy and switch from one model to the other. Hot redundancy can use redundant physical interfaces, slave ATM switches with Y redundancy, and redundant LSCs. This enables parallel paths and near-instant failover. If your resources are limited, you can implement warm redundancy, which uses only redundant LSCs. When one controller fails, the backup controller requires some reroute time. As your network grows, you can switch from hot to warm redundancy and back, without bringing down the entire network.

Other redundancy models require complex hardware and software configurations, which are difficult to alter when you change the network configuration. You must manually change the connection routing software from hot standby mode to warm standby mode.

LSC Redundancy Provides an Easy Migration from Standalone LSCs to Redundant LSCs

You can migrate from a standalone LSC to a redundant LSC and back again without affecting network operations. Because the LSCs work independently, you can add a redundant LSC without interrupting the other LSC.

LSC Redundancy Allows Configuration Changes in a Live Network

The hot LSC redundancy model provides two parallel, independent networks. Therefore, you can disable one LSC without affecting the other LSC. This feature has the following benefits:

- LSC redundancy model facilitates configuration changes and updates. After you finish with configuration changes or image upgrades to the LSC, you can add the LSC back to the network and resume the LSC redundancy model.
- The redundancy model protects the network during partitioning of the ATM switch. You can disable one path and perform partitioning on that path. While you are performing the partitioning, data uses the other path. The network is safe from the effects of the partitioning, which include breaking/establishing LVC connections.

LSC Redundancy Provides Fast Reroute in IP+ATM Networks

The hot LSC redundancy model offers redundant paths for every destination. Therefore, reroute recovery is very fast. Other rerouting processes in IP+ATM networks require many steps and take more time.

In normal IP+ATM networks, the reroute process consists of the following steps:

- Detecting the failure
- Converging the Layer 2 routing protocols
- Completing label distribution for all destinations
- Establishing new connections for all destinations

After this reroute process, the new path is ready to transfer data. Rerouting data using this process takes time.

The hot LSC redundancy method allows you to quickly reroute data in IP+ATM networks without using the normal reroute process. When you incorporate hot LSC redundancy, you create parallel paths. Every destination has at least one alternative path. If a device or link along the path fails, the data uses the other path to reach its destination. The hot LSC redundancy model provides the fastest reroute recovery time for IP+ATM networks.

LSC Redundancy Restrictions

Hot LSC Redundancy Restrictions

The following list explains the items you need to consider when implementing hot LSC redundancy:

- LSC hot redundancy needs parallel paths. Specifically, there must be the capacity for at least two end-to-end parallel paths traveling from each source to each destination. Each path is controlled by one of a pair of redundant LSCs.
- Label switch paths (LSPs) for the destinations are initiated from the Edge LSR. The Edge LSR initiates multiple paths for a destination only if it has parallel paths to its next hop. Therefore, it is important to have parallel paths from the Edge LSR. You can achieve parallel paths by having two physical links from the Edge LSR or by having two separate VP tunnels on one link.
- Hot redundancy protection extends from the Edge LSR only as far as parallel paths are present. So, it is best if parallel paths are present throughout the entire network.

- Hot redundancy increases the number of VCs used in the network. Each physical link with two VSI partitions has twice the number of VCs used than would otherwise be the case. Various techniques can be used to alleviate VC usage. The use of unnumbered links (“ip unnumbered” in the IOS link configuration) reduces the number of routes in the routing table and hence the number of VCs required. On the LSCs, you can use the command **mpls atm disable-headend-vc** to disable Edge LSR functionality on the LSC and also reduce the number of VCs used. The **mpls request-labels for** command with an access list also restricts the creation of LVCs.

Warm LSC Redundancy Restrictions

The following list explains the items you need to consider when implementing warm LSC redundancy:

- LSC warm redundancy needs a single active path between the source and destination. However, there is also a requirement for end-to-end parallel paths, as in the hot redundancy case. Only one path has an active LSP for the destination. In the event of the failure, the other path is established, with some delay due to rerouting.
- The number of VCs in the network does not change with the warm redundancy.
- Hot LSC redundancy achieves failure recovery with little loss of traffic. However, hot redundancy doubles the VC requirements in the network. Warm LSC redundancy requires the same number of VCs as a similar network without LSC redundancy. However, traffic loss due to a failure is greater; traffic may be lost for a period of seconds during rerouting.



Note

The precise traffic loss depends on the type of failure. If the failure is in an LSC, the LSPs controlled by that LSC typically remain connected for some time. Traffic can still flow successfully on the “failed” path until the Edge LSRs switch all traffic to the alternate path (which might occur tens of seconds later, depending on routing protocol configuration). The only traffic loss might occur in the Edge LSR when traffic changes to the new path, which typically takes a few milliseconds or less.

Configuring LSC Redundancy

To make an LSC redundant, you can partition the resources of the slave ATM switch, implement a parallel VSI model, assign redundant LSCs to each switch, and create redundant LSRs. The following sections explain each of these steps.

Partitioning the Resources of the ATM Switch

In the LSC redundancy model, two LSCs control different partitions of the ATM switch. When you partition the ATM switch for LSC redundancy, use the following guidelines:

- Make the MPLS partitions identical. If you create two partitions, make sure both partitions have the same amount of resources. (You can have two MPLS VSI partitions per switch.) Use the **cnfrsrc** command to configure the partitions.
- If the partitions are on the same switch card, perform the following:
 - Create different control VCs for each partition. For example, there can be only one (0, 32) control VC on the XTagATM interface. To map two XTagATM interfaces on the same ATM switch interface, use a different control VC for the second LSC. Use the **mpls atm control-vc** command.
 - Create the LVC on the XTagATM interfaces using nonintersecting VPI ranges. Use the **mpls atm vpi** command.

- Specify the bandwidth information on the XTagATM interfaces. Normally, this information is read from the slave ATM switch. When you specify the bandwidth on the XTagATM interface, the value you enter takes precedence over the switch-configured interface bandwidth.
- Configure the logical channel number (LCN) ranges for each partition according to the expected number of connections.

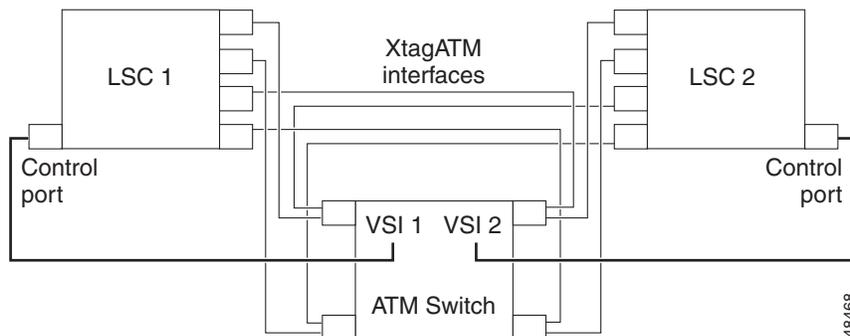
See the documentation on the Cisco BPX 8600 series or Cisco IGX 8400 series switches for more information about configuring the slave ATM switch.

Implementing the Parallel VSI Model

The parallel VSI model means that the physical interfaces on the ATM switch are shared by more than one LSC. For instance, LSC1 maps VSI slave interfaces 1 to N to the ATM switch's physical interfaces 1 to N. LSC2 maps VSI slave interfaces to the ATM switch's physical interfaces 1 to N. LSC1 and LSC2 share the same physical interfaces on the ATM switch. With this mapping, you achieve fully meshed independent masters.

Figure 23 shows four ATM physical interfaces mapped as four XTagATM interfaces at LSC1 and LSC2. Each LSC is not aware that the other LSC is mapped to the same interfaces. Both LSCs are active all the time. The ATM switch runs the same VSI protocol on both partitions.

Figure 23 XTagATM Interfaces

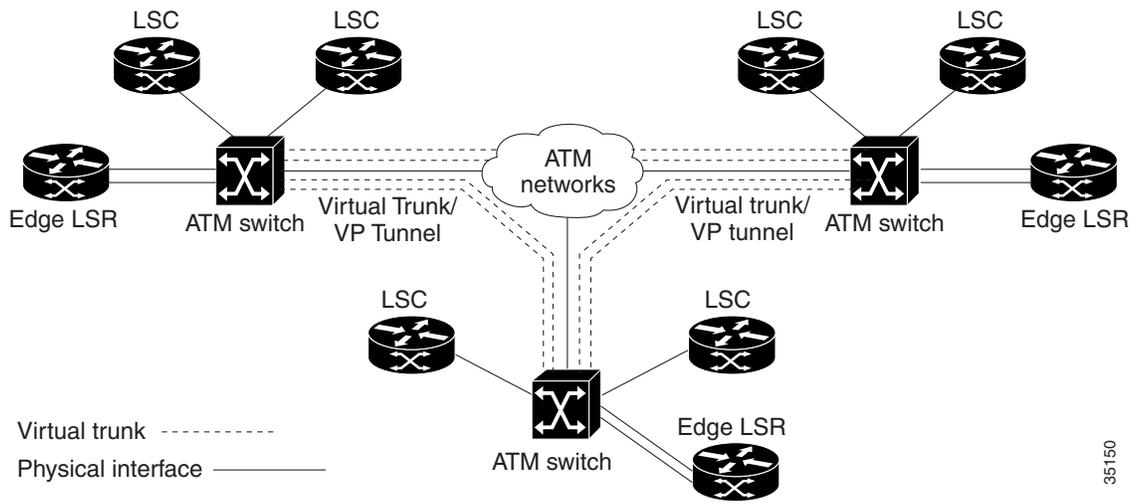


Adding Interface Redundancy

To ensure reliability throughout the LSC redundant network, you can also implement:

- Redundant interfaces between the Edge LSR and the ATM-LSR. Most Edge LSRs are colocated with the LSCs. Creating redundant interfaces between the Edge LSRs and the ATM LSRs reduces the chance of a disruption in network traffic by providing parallel paths.
- Redundant virtual trunks and VP tunnels between slave ATM switches. To ensure hot redundancy between the ATM switches, you can create redundant virtual trunks and VP tunnels. See Figure 24.

Figure 24 Interface Redundancy

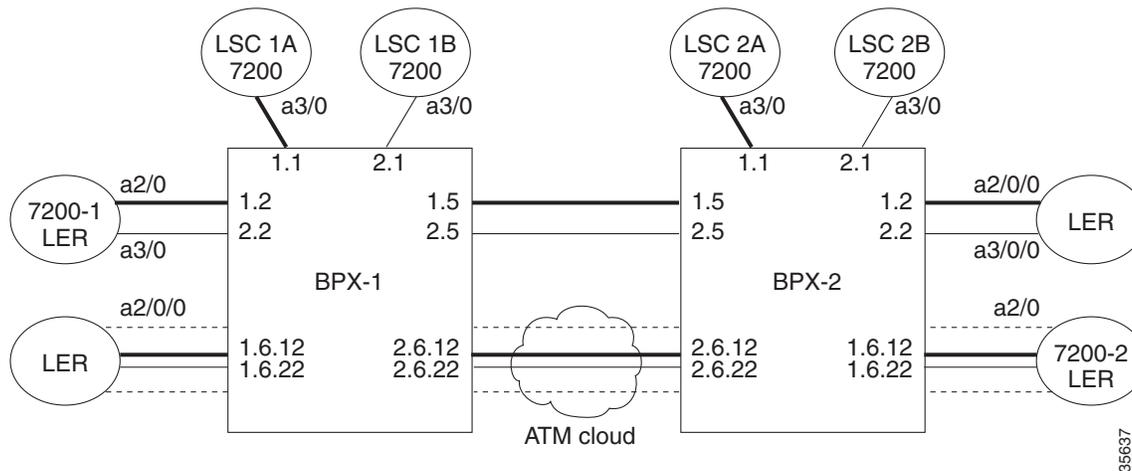


95150

Configuration Example: Configuring LSC Hot Redundancy

The network topology shown in Figure 25 incorporates two ATM-LSRs in an MPLS network. This topology includes two LSCs on each BPX node and four Edge LSRs.

Figure 25 ATM-LSR Network Configuration Example



The following configuration examples show the label-switching configuration for both standard downstream-on-demand interfaces and downstream-on-demand over a VP-tunnel. The difference between these two types of configurations is:

- Standard interface configuration configures a VPI range of one or more VPIs while LDP control information flows in PVC 0,32.
- VP-tunnel, on the other hand, configures a single VPI (for example, vpi 12) and uses an mpls atm control-vc of vpi,32 (i.e. 12,32). You can use a VP-tunnel to establish label-switching neighbor relationships through a private ATM cloud.

The following configuration examples are provided in this section.



Note

For the Cisco IGX switch, use the following commands:

```
extended-port atm1/0 descriptor 0.x.x.0
tag-control-protocol vsi slaves 32 id x
ip route-cache cef
```



Note

In the following configuration examples for the LSCs, you can use the **mpls request-labels for** command instead of the **mpls atm disable-headend-vc** command.

Configuration for LSC 1A

7200 LSC 1A:

```
ip cef
!
mpls atm disable-headend-vc
!
interface loopback0
```

```

        ip address 172.103.210.5 255.255.255.255
    !
interface ATM3/0
no ip address
tag-control-protocol vsi id 1
ip route-cache cef
!
interface XTagATM12
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 1.2
    mpls atm vpi 2-5
    mpls ip
!
interface XTagATM15
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 1.5
    mpls atm vpi 2-15
    mpls ip
!
interface XTagATM1612
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 1.6.12
    mpls atm vp-tunnel 12
    mpls ip
!
interface XTagATM2612
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 2.6.12
    mpls atm vp-tunnel 12
    mpls ip

```

Configuration for LSC 1B

7200 LSC 1B:

```

ip cef
!
mpls atm disable-headend-vc
!
!
interface loopback0
    ip address 172.103.210.6 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi id 2
ip route-cache cef
!
interface XTagATM22
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 2.2
    mpls atm vpi 2-5
    mpls ip
!
interface XTagATM25
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 2.5
    mpls atm vpi 2-15
    mpls ip
!
interface XTagATM1622
    ip unnumbered loopback0

```

```

        extended-port ATM3/0 bpx 1.6.22
        mpls atm vp-tunnel 22
        mpls ip
    !
interface XTagATM2622
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 2.6.22
    mpls atm vp-tunnel 22
    mpls ip

```

Configuration for LSC 2A

7200 LSC 2A:

```

ip cef
!
mpls atm disable-headend-vc
!
interface loopback0
    ip address 172.103.210.7 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi id 1
ip route-cache cef
!
interface XTagATM12
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 1.2
    mpls atm vpi 2-5
    mpls ip
!
interface XTagATM15
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 1.5
    mpls atm vpi 2-15
    mpls ip
!
interface XTagATM1612
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 1.6.12
    mpls atm vp-tunnel 12
    mpls ip
!
interface XTagATM2612
    ip unnumbered loopback0
    extended-port ATM3/0 bpx 2.6.12
    mpls atm vp-tunnel 12
    mpls ip

```

Configuration for LSC 2B

7200 LSC 2B:

```

ip cef
!
mpls atm disable-headend-vc
!
interface loopback0
    ip address 172.103.210.8 255.255.255.255
!
interface ATM3/0

```

```

no ip address
tag-control-protocol vsi id 2
ip route-cache cef
!
interface XTagATM22
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.2
  mpls atm vpi 2-5
  mpls ip
!
interface XTagATM25
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.5
  mpls atm vpi 2-15
  mpls ip
!
interface XTagATM1622
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 1.6.22
  mpls atm vp-tunnel 22
  mpls ip
!
interface XTagATM2622
  ip unnumbered loopback0
  extended-port ATM3/0 bpx 2.6.22
  mpls atm vp-tunnel 22
  mpls ip

```

Configuration for BPX-1 and BPX-2

BPX-1 and BPX-2:

```

uptrk 1.1
addshelf 1.1 vsi 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
upln 1.2
upport 1.2
cnfrsrc 1.2 256 252207 y 1 e 512 6144 2 5 26000 100000
uptrk 1.5
cnfrsrc 1.5 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.6.12
cnftrk 1.6.12 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,
RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 12
cnfrsrc 1.6.12 256 252207 y 1 e 512 6144 12 12 26000 100000
uptrk 1.6.22
cnftrk 1.6.22 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,
RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 22
cnfrsrc 1.6.22 256 252207 y 2 e 512 6144 22 22 26000 100000
uptrk 2.1
addshelf 2.1 vsi 2 2
cnfrsrc 2.1 256 252207 y 2 e 512 6144 2 15 26000 100000
upln 2.2
upport 2.2
cnfrsrc 2.2 256 252207 y 2 e 512 4096 2 5 26000 100000
uptrk 2.5
cnfrsrc 2.5 256 252207 y 2 e 512 6144 2 15 26000 100000
uptrk 2.6.12
cnftrk 2.6.12 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,
RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 12
cnfrsrc 2.6.12 256 252207 y 1 e 512 6144 12 12 26000 100000
uptrk 2.6.22
cnftrk 2.6.22 110000 N 1000 7F V,TS,NTS,FR,FST,CBR,NRT-VBR,ABR,

```

```
RT-VBR N TERRESTRIAL 10 0 N N Y Y Y CBR 22
cnfrsrc 2.6.22 256 252207 y 2 e 512 6144 22 22 26000 100000
```

**Note**

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for instance, XTagATM11).

Configuration for Edge LSR 7200-1

7200-1 Edge LSR:

```
ip cef
!
interface loopback0
    ip address 172.103.210.1 255.255.255.255
!
interface ATM2/0
    no ip address
!
interface ATM2/0.12 mpls
    ip unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip
!
interface ATM3/0
    no ip address

interface ATM3/0.22 mpls
    ip unnumbered loopback 0
    mpls atm vpi 2-5
    mpls ip
```

Configuration for Edge LSR-1

Edge LSR:

```
ip cef distributed
!
interface loopback0
    ip address 172.103.210.2 255.255.255.255
!
interface ATM2/0/0
    no ip address
!
interface ATM2/0/0.1612 mpls
    ip unnumbered loopback0
    mpls atm vp-tunnel 12
    mpls ip
!
interface ATM2/0/0.1622 mpls
    ip unnumbered loopback0
    mpls atm vp-tunnel 22
    mpls ip
```

Configuration for Edge LSR-2

Edge LSR:

```
ip cef distributed
```

```

!
interface loopback0
  ip address 172.103.210.3 255.255.255.255
!
interface ATM2/0/0
  no ip address
!
interface ATM2/0/0.12 mpls
  ip unnumbered loopback0
  mpls atm vpi 2-5
  mpls ip
!!
interface ATM3/0/0
  no ip address
!
interface ATM3/0/0.22 mpls
  ip unnumbered loopback0
  mpls atm vpi 2-5
  mpls ip

```

Configuration for Edge LSR 7200-2

7200-2 Edge LSR:

```

ip cef
!
interface loopback0
  ip address 172.103.210.4 255.255.255.255
!
interface ATM2/0
  no ip address
!
interface ATM2/0.1612 mpls
  ip unnumbered loopback0
  mpls atm vp-tunnel 12
  mpls ip
!
interface ATM2/0.1622 mpls
  ip unnumbered loopback0
  mpls atm vp-tunnel 22
  mpls ip

```

Configuration Example: Configuring LSC Warm Standby Redundancy

You can implement the configuration of LSC warm standby redundancy by configuring the redundant link for either a higher routing cost than the primary link or configuring a bandwidth allocation that is less desirable. You need to perform this only at the Edge LSR nodes, because the LSCs are configured to disable the creation of headend VCs, which reduces the LVC overhead.

Configuration Example: Configuring an Interface Using Two VSI Partitions

A special case may arise where a network topology can only support a neighbor relationship between peers using a single trunk or line interface. To configure the network, use the following procedure:

Step 1 Configure the interface to use both VSI partitions. The VSI partition configuration for the interface must be made with no overlapping vp space. For instance, for interface 2.8 on the ATM LSR, the following configuration is required:

```
uptrk 2.8
cnfrsrc 2.8 256 252207 y 1 e 512 6144 2 15 26000 100000
cnfrsrc 2.8 256 252207 y 2 e 512 6144 16 29 26000 100000
```

Thus partition 1 will create LVCs using VPIs 2-15 and partition 2 will create LVCs using VPIs 16-29.

Step 2 Configure the control-vc. Each LSC requires a control VC (default 0,32); however, only one LSC can use this default control-vc for any one trunk interface. The following command forces the control VC assignment:

```
mpls atm control-vc <vpi> <vci>
```

Therefore, LSC 1 XTagATM28 can use the default control-vc 0/32 (but it is suggested that you use 2/32 to reduce configuration confusion) and the LSC 2 XTagATM28 should use control-vc 16/32.



Note

For the Cisco IGX switch, use the following commands:
extended-port atm1/0 descriptor 0.x.x.0
tag-control-protocol tag-control-protocol vsi slaves 32 id x
ip route-cache cef

The following example shows the configuration steps:

LSC1:

```
interface XTagATM2801
 ip unnumbered loopback0
 extended-port ATM3/0 bpx 2.8
 mpls atm vpi 2-15
 mpls atm control-vc 2 32
 mpls ip
```

LSC2:

```
interface XTagATM2802
 ip unnumbered loopback0
 extended-port ATM3/0 bpx 2.8
 mpls atm vpi 16-29
 mpls atm control-vc 16 32
 mpls ip
```

Feature 3: Reducing the Number of Label Switch Paths Created in an MPLS Network

You can reduce the number of LSPs created in an MPLS network by disabling LSPs from being created from an edge LSR or LSC to a destination IP address. Use the **mpls request-labels for** command. Specify the destination IP addresses that you want to disable from creating LSPs. This command allows you to permit creation of some LSPs, while preventing the creation of others.

Using an Access List to Disable Creation of LSPs to Destination IP Addresses

You can prevent LSPs from being created between Edge LSRs and LSCs. This helps prevent the unnecessary use of LVC resources in a slave ATM switch. You use the `mpls request-labels for` command with an access list to disable the creation of the LSPs.

Some LSPs are often unnecessary between some Edge LSRs in an MPLS network. Every time a new destination is created, LSPs are created from all Edge LSRs in the MPLS network to the new destination. You can create an access list at an Edge LSR or LSC to restrict the destinations for which a downstream-on-demand request is issued.

For example, [Figure 26](#) is an MPLS ATM network that consists of the following elements:

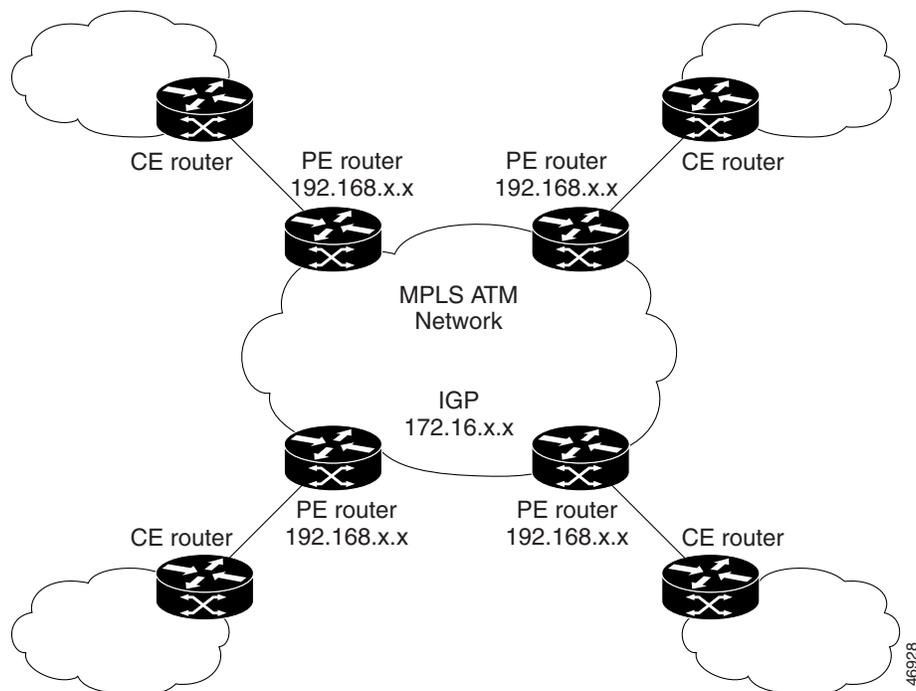
- The PE routers in the virtual private network require LSPs to communicate with each other.
- All the PE routers are in network 1 (192.168.x.x).
- All the IGP IP addresses are in network 2 (172.16.x.x).
- If numbered interfaces are required (for network management or other purposes), they are placed in network 2 (172.16.x.x).

Use `mpls request-labels for` commands to accomplish the following tasks:

- Allow the PE routers in network 1 to create LSPs and communicate with each other.
- Prevent LSPs from being created in network 2.

Performing these tasks reduces the number of LSPs in the MPLS ATM cloud, which reduces the VC usage in the cloud.

Figure 26 Sample MPLS ATM Network

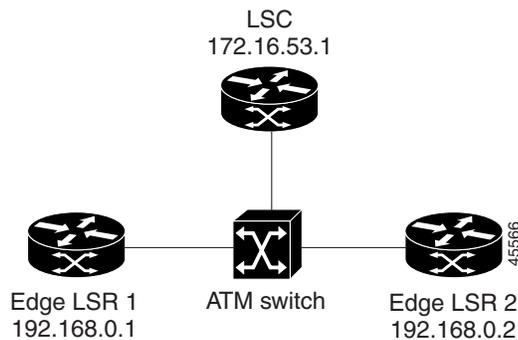


**Note**

When using access lists to prevent the creation of headend LVCs or LSPs, do not disable the LSC from acting as an Edge LSR with the **mpls atm disable-headend-vc** command, which prevents all LSPs from being established.

The following examples of the **mpls request-labels for** command use [Figure 27](#) as a basis. The examples show different ways to disable the creation of LSPs from the LSC to the Edge LSR, and from the Edge LSRs to the LSC.

Figure 27 Sample Configuration for *mpls request-labels for* Command



Using a Numbered Access List

The following examples use a numbered access list to restrict creation of LSPs.

Preventing LSPs from the LSC to the Edge LSRs

The following example prevents LSPs from being established from the LSC to all 192.x.x.x destinations. However, transit LSPs are allowed between 192.x.x.x destinations. Add the following commands to the LSC configuration:

```
mpls request-labels for 1
access-list 1 deny 192.168.0.0 0.255.255.255
access-list 1 permit any
```

Preventing LSPs from the Edge LSRs to the LSC

The following example prevents headend LVCs from being established from Edge LSR 1 and Edge LSR 2 to the LSC (172.16.x.x). However, transit LSPs are allowed between 192.168.x.x destinations. Add the following commands to the Edge LSR 1 and 2 configurations:

```
mpls request-labels for 1
access-list 1 deny 172.16.0.0 0.255.255.255
access-list 1 permit any
```

Using a Named Access List

The following examples use a named access list to perform the same tasks as the previous examples:

```
mpls request-labels for nolervcs
ip access-list standard nolervcs
deny 192.168.0.0 0.255.255.255
permit any
```

```
mpls request-labels for nolervcs
ip access-list standard nolervcs
deny 172.16.0.0 0.255.255.255
permit any
```

Specifying Exact Match IP Addresses with an Access List

The following examples use exact IP addresses to perform the same tasks as the previous examples:

```
mpls request-labels for 1
access-list 1 deny 192.168.0.1 0.0.0.0
access-list 1 deny 192.168.0.2 0.0.0.0
access-list 1 permit any
```

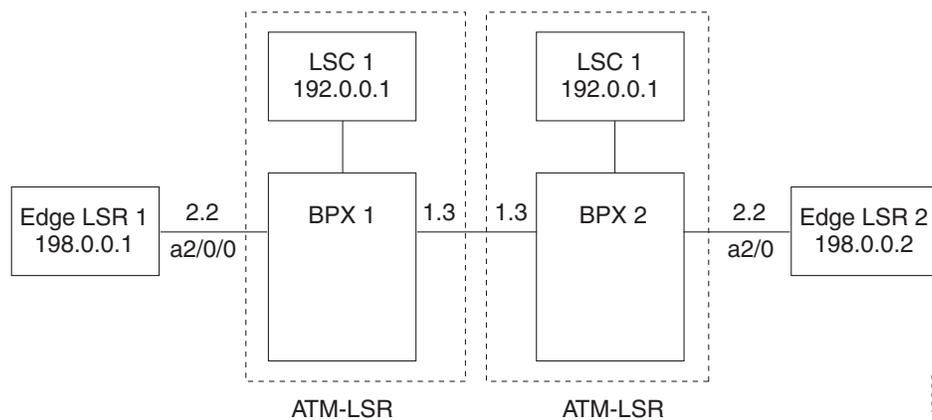
```
mpls request-labels for 1
access-list 1 deny 172.16.53.1 0.0.0.0
access-list 1 permit any
```

Configuration Example: Using an Access List to Limit Headend VCs

The following example shows how to use an access list to control the creation of headend VCs in an MPLS network, which allows the network to support more destinations.

Figure 28 shows two Edge LSRs and two ATM-LSRs. In the configuration, only LSPs between Edge LSRs are required to provide label switched paths. Other LSPs are not essential. The LSPs between LSCs and between the LSCs and the Edge LSRs are often unused and required only for monitoring and maintaining the network. In such cases the IP forwarding path is sufficient.

Figure 28 Sample MPLS Network



In networks that require connections only between Edge LSRs, you can use the access list to eliminate the creation of unnecessary LSPs. This allows LVC resources to be conserved so that more Edge LSR connections can be supported.

To prevent creation of LSPs between LSCs, create an access list that denies all 172.16.0.0/24 addresses. Then, to prevent creation of LVCs from the LSCs to the Edge LSRs, create an access list that denies all 192.168.0.0/24 addresses. The configuration examples for LSC 1 and 2 show the commands for performing these tasks.

To prevent creation of LVCs from the Edge LSRs to LSCs, create an access list at the Edge LSRs that denies all 172.16.0.0/24 addresses. The configuration examples for Edge LSR 1 and 2 show the commands for performing this task.

Configuration for LSC 1

7200 LSC 1:

```

ip cef
!
mpls request-labels for acl_lsc
ip access-list standard acl_lsc
deny 172.16.0.0 0.255.255.255
deny 192.168.0.0 0.255.255.255
permit any
!
interface loopback0
 ip address 172.16.0.1 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
 extended-port ATM3/0 bpx 1.3
 ip unnumbered loopback0
 mpls atm vpi 2-15
 mpls ip
!
interface XTagATM22
 extended-port ATM3/0 bpx 2.2
 ip unnumbered loopback0
 mpls atm vpi 2-5
 mpls ip

```

Configuration for BPX 1 and BPX 2

BPX 1 and BPX 2:

```

uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3
cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000

```



Note

For the shelf controller, you must configure a VSI partition for the slave control port interface (**addshelf 1.1, cnfrsrc 1.1...**). However, do not configure an XTagATM port for the VSI partition (for instance, XTagATM11).

Configuration for LSC 2

7200 LSC 2:

```

ip cef
!
mpls request-labels for acl_lsc
ip access-list standard acl_lsc
deny 172.16.0.0 0.255.255.255
deny 192.168.0.0 0.255.255.255
permit any
!
interface loopback0
 ip address 172.16.0.2 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
 extended-port ATM3/0 bpx 1.3
 ip unnumbered loopback0
 mpls atm vpi 2-15
 mpls ip
!
interface XTagATM22
 extended-port ATM3/0 bpx 2.2
 ip unnumbered loopback0
 mpls atm vpi 2-5
 mpls ip
!

```

Configuration for Edge LSR 1

LSR 1:

```

ip cef distributed
!
mpls request-labels for acl_ler
ip access-list standard acl_ler
deny 172.16.0.0 0.255.255.255
permit any
!
interface loopback 0
 ip address 192.168.0.1 255.255.255.255
!
interface ATM2/0/0
 no ip address
!
interface ATM2/0/0.22 mpls
 ip unnumbered loopback 0
 mpls atm vpi 2-5
 mpls ip

```

Configuration for Edge LSR 2

7200 LSR 2:

```

ip cef
!
mpls request-labels for acl_ler

```

```
ip access-list standard acl_1er
deny 172.16.0.0 0.255.255.255
permit any
!
interface loopback 0
 ip address 192.168.0.2 255.255.255.255
!
interface ATM2/0
 no ip address
!
interface ATM2/0.22 mpls
 ip unnumbered loopback 0
 mpls atm vpi 2-5
 mpls ip
```

Feature 4: Differentiated Services and MPLS QoS Multi-VCs

Quality of service (QoS) refers to the ability of a network to provide better service to selected network traffic over various underlying technologies including Frame Relay, ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks. In particular, QoS features provide better and more predictable network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, and setting traffic priorities across the network.

A service model, also called a level of service, describes a set of end-to-end QoS capabilities. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. Differentiated services is a service model supported by Cisco IOS QoS software that can provide end-to-end QoS.

The Multiprotocol Label Switching quality of service (MPLS QoS) mechanism is a feature for performing differentiated services over ATM. The MPLS QoS Multi-VC mode enhances general MPLS QoS features by enabling users to map the experimental (EXP) field value of an MPLS label to an ATM virtual circuit (VC) to create sets of labeled virtual circuits (LVCs). Each set consists of multiple LVCs, and each LVC is treated as a member of the set.

Differentiated Services and Quality of Service

Differentiated service (DiffServ) is a multiple service model that can satisfy differing QoS requirements. However, unlike the integrated service model, an application using differentiated service does not explicitly signal the router before sending data.

Two different acronyms are used for differentiated services and both are commonly used in other documents. “DiffServ” is used most commonly, and refers to differentiated services in general. “DS” is the name given specifically to the bits in the IP headers used by DiffServ.

For differentiated service, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the IP Precedence bit settings in IP packets. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queuing.

The differentiated service model is used for several mission-critical applications and for providing end-to-end QoS. Typically, this service model is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

Cisco IOS QoS includes the following features that support the differentiated service model:

- Committed access rate (CAR), which performs packet classification through IP Precedence and QoS group settings. CAR performs metering and policing of traffic, providing bandwidth management.
- Intelligent queuing schemes such as WRED and WFQ and their equivalent features on the Versatile Interface Processor (VIP), which are VIP-Distributed WRED and VIP-Distributed WFQ. These features can be used with CAR to deliver differentiated services.

The DiffServ approach to QoS divides network traffic into a small number of classes and allocates resources on a per-class basis. DiffServ can be viewed as an incremental approach to QoS.

DiffServ Per-Hop Behaviors

DiffServ networks use queuing technologies such as weighted fair queuing (WFQ) to provide differential service to the different classes of service (CoS). Link-by-link engineering of WFQ parameters is the approach suggested by the IETF DiffServ Working Group.

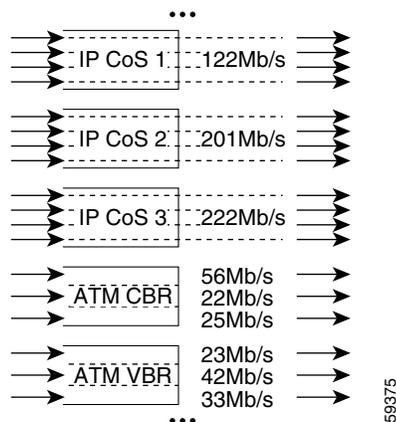
The treatment of a particular CoS on a particular link (or “hop”), using technologies such as weighted fair queuing, is referred to as a per-hop behavior (PHB). Cisco supports engineering of per-hop behaviors on links in both ATM MPLS and packet-based MPLS networks, as well as ordinary IP networks. The principles are the same in all network types, although there are differences in the way CoS information is carried in packets for different networks.

DiffServ Classes and Cisco IP+ATM Switches

Engineering of DiffServ networks leads to specifications of required bandwidths for various classes of service on various links of the network. This is quite different from traditional per-VC bandwidth management in ATM networks.

As shown in [Figure 29](#), class-based queuing involves a separate queue in the ATM switch for each CoS. Cells from all LVCs of each CoS are queued in a single queue for that CoS. The bandwidth parameters of a CoS on a link are set directly on the CoS queue. The only parameter signalled for each LVC is the CoS for the LVC. This means that the ATM MPLS control component is used unchanged, except that multiple LVCs are set up for each destination: one LVC per destination per CoS.

Figure 29 Per-VC Service and CoS in Cisco IP + ATM Switches



Cisco IP+ATM switches support DiffServ for MPLS traffic, alongside ATM Forum Traffic Management types for PVCs and SVCs. Each DiffServ or ATM Forum Traffic Management type gets its own “class of service buffer.” Per-VC queuing can be used in addition to the class of “class of service buffers” and this is done for ATM Forum Traffic Management types. Weighted fair queuing is used to assign bandwidths to the IP class of service buffers. This means that the IP classes share bandwidth.

Using class-based queuing instead of per-VC queuing for the IP traffic has several advantages:

- The number of parameters programmed into the network is much smaller with class-based queuing: if a network has N nodes, the number of parameters required is proportional to N^2 with per-VC queuing, but proportional to N with class-based queuing.
- Class-based queuing is fairer, given approximate information. This is important because engineering of an IP network is based on estimates and models of customer traffic. With class-based queuing, premium-class traffic from any origin to any destination gets preferential access to a premium-class bandwidth left spare from other origin-destination pairs. This is much harder to achieve if bandwidths are assigned to individual origin-destination LVCs.
- Class-based queuing can be used on any link types. Link types include those that do not support virtual circuits: PPP-over-SDH and WDM. Use of class-based queuing helps make a network flexible and open to future changes in technology without major changes in operations, administration, and management. Cisco already makes switch-routers with ATM, PPP-over-SDH, and WDM interfaces.
- Class-based queuing works better with VC merge than per-VC queuing. Per-VC queuing negates the advantages of VC merge in improving signaling scale. If per-LVC queuing were used, each LVC in the tree of LVCs merging to a given destination would need a bandwidth assigned to it according to the sum of bandwidth requirements merging in from other branches. Any addition or change made to the bandwidths of the merging VCs would create a ripple of signaling through the network. This negates one of the important advantages of VC merge, namely that VC merge removes the requirement for end-to-end signaling for most LVCs.
- Even if class-based queuing is used, changes to class-based bandwidths will be required as bandwidth requirements change. However these can be dealt with as a network provisioning issue on a time-frame of at least hours or days. Class-based queuing does not require the real-time QoS signaling overheads of per-VC queuing. Furthermore, the granularity of changes with class-based queuing is per-link; with per-VC queuing, the granularity is per-VC. This is another example of how class-based queuing is more scalable.

For these reasons, Cisco strongly recommends that networks supporting IP services are engineered using class-based queuing.

Requirements for Differential Services Approach to QoS

Good quality of service can be provided to connectionless IP traffic, on MPLS networks in particular. The process involves the following:

- Enforcement of access contracts at the edge of a network using Cisco CAR
- Using the access contracts as a basis for modeling traffic
- Optional refinement of traffic models based on operation of a network
- Setting of the links' queuing parameters according to the traffic models
- Offering SLAs of an appropriate form and strength for a connectionless IP service
- Service admission control

Configuring Multi-VCs

The Multiprotocol Label Switching quality of service (MPLS QoS) mechanism is a feature for performing differentiated services over ATM. It allows the ATM network to treat different packets based on the EXP (experimental) field (also called CoS) of the MPLS header which has the same properties, and which can be mapped to IP precedence. You can configure multiple VCs that have different QoS characteristics between any pair of ATM-connected routers.

Every label switch router (LSR) has a corresponding number of virtual circuits (VCs)—from one to four—for the same destination, hence the term “multi-VC.” These parallel label virtual circuits (LVCs) are set up automatically by the upstream edge router using the Label Distribution Protocol. Each set consists of multiple LVCs, and each LVC is treated as a member of the set.

For more detailed information on configuring multi-VCs, refer to the following document:

[MPLS QoS Multi-VC Mode for PA-A3](#)

Setting Up LVCs

When you configure multi-VC support, four LVCs for each destination are created by default that map to MPLS QoS. [Table 7](#) shows the LVC to MPLS QoS mapping.

Table 7 LVC to MPLS QoS Mapping

Label Virtual Circuit Type	Class of Service	IP Type of Service
Available	0	0,4
Standard	1	1,5
Premium	2	2,6
Control	3	3, 7

To set up four default LVCs (with default mapping), you add the following instruction to the ATM subinterface configuration of the Edge LSRs:

```
mpls atm multi-vc
```

The parallel LVCs are set up automatically on the ATM switches.

Optionally Setting the MPLS Experimental Field Value

The ability to optionally set the MPLS EXP field of the label header upon entry of a customer IP packet into an MPLS network has no direct connection to the MPLS QoS multi-VC mode feature per se. However, the ability to manipulate the EXP field provides flexibility to preserve the IP precedence value in the IP type-of-service (ToS) byte in the header of an incoming IP packet. The service provider can manage queues or select LVCs based on the value of the EXP field.

You can set the MPLS experimental field (EXP) value in customer IP packets arriving at the provider edge router by means of modular QoS CLI commands or CAR commands executed on that edge router.

Using Modular QoS CLI to Configure Ingress Label Switching Router

To use the modular QoS CLI to configure the ingress LSR appropriately for multi-VC mode functionality, perform the following steps:

-
- Step 1** Configure a class map to classify IP packets according to their IP precedence.
 - Step 2** Configure a policy map to mark MPLS packets (that is, to write their classification into the MPLS EXP field).
 - Step 3** Configure the input interface of the ingress router to attach the service policy.
-

In the following example, all packets that contain IP precedence 4 are matched by the class-map name IP_prec4:

```
Router(config)# class-map IP_prec4
Router(config-c-map)# match ip precedence 4
Router(config-c-map)# end
```

In the following example, the MPLS EXP field of each IP packet that matches class-map IP_prec4 is set to a value of 5:

```
Router(config)# policy-map set_experimental_5
Router(config-p-map)# class IP_prec4
Router(config-p-map-c)# set mpls experimental 5
Router(config-p-map-c)# end
```

In the following example, the service policy set_experimental_5 is attached to the specified Ethernet input interface (et 1/0/0):

```
Router(config)# interface et 1/0/0
Router(config-if)# service-policy input set_experimental_5
Router(config-if)# end
```

Using CAR to Configure an Ingress Label Switching Router

To classify the packets on the ingress Edge LSR, you can use MPLS QoS committed access rate (CAR) service to set the EXP field of the MPLS header to the desired value. To use CAR to configure the ingress LSR for multi-VC mode functionality, perform the following steps:

-
- Step 1** Configure an IP rate-limit access list for classifying IP packets according to their IP precedence.
 - Step 2** Configure a rate-limit on an input interface to mark the MPLS packets (to write the packet's classification into the MPLS EXP field).
-

In the following example, all packets containing IP precedence value 4 are matched by the rate-limit access list 24:

```
Router(config)# access-list rate-limit 24 4
Router(config)# end
```

In the following example, the MPLS EXP field is set to 4 on output of packets if input IP packets match the access-list and conform to the packet rate. The MPLS EXP field is set to 0 if packets match access list 24 and exceed the input rate.

```
Router(config)# interface et 1/0/0
Router(config-if)# rate-limit input access-group rate-limit 24 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
Router(config-if)# end
```

**Note**

You can also use the **mpls atm vpi 2-4** command, but it is not mandatory to specify which virtual path identifiers (VPIs) will be used for MPLS.

You need to configure **ip cef (ip cef distributed)** on a Cisco 7200) on the general configuration of the routers before you configure CAR.

Configuring MPLS QoS in the Core of an ATM Network

To configure MPLS QoS in the core of an ATM network, perform the following steps:

-
- Step 1** Configure an ATM MPLS subinterface on the core router and enable multi-VC mode on that subinterface.
 - Step 2** Optionally, create an MPLS QoS map and associate that map with the core router.
-

The default for the multi-VC mode creates four LVCs (available, standard, premium, and control) for each MPLS destination.

If you do not choose to use the default for configuring LVCs, you can configure fewer LVCs by using the QoS map function.

Configuring Queuing Functions on Router Output Interfaces

To configure class-based weighted fair queuing (CBWFQ) and weighted random early detection (WRED) functionality on a Cisco 7200 series router interface or a Cisco MGX 8850 switch with the Cisco RPM-PR card interface, perform the following steps:

-
- Step 1** Create a class map and associate it with an IP type of service to match on a packet.
 - Step 2** Create a policy map to match with the class map.
 - Step 3** Assign a CBWFQ to the policy map to act on the packet.
 - Step 4** Assign a WRED to the policy map to act on the packet.
 - Step 5** Specify an interface and assign the policy map on the interface.
-

Setting the ATM-CLP Bit on Enhanced ATM Port Adapter Interfaces

To set the ATM-CLP bit in ATM cells exiting from an enhanced ATM port adapter interface incorporated into a Cisco 7200 router or a Cisco MGX RPM-PR (in a Cisco MGX 8850 or 8890 switch), perform the following steps:

-
- Step 1** Create a class map and associate it with an IP type of service to match on a packet.
 - Step 2** Create a policy map to match with the class map.
 - Step 3** Configure MPLS packets matching this class to have the CLP bit set in the outgoing ATM cells.
 - Step 4** Specify an interface and assign the policy map on the interface.
-

Verifying MPLS QoS Operation

To verify the operation of MPLS QoS, issue the following commands to view information about the switching interfaces, the specified QoS map used to assign a quantity of VCs, and the prefix map used to assign a QoS map to network prefixes that match a standard IP access list.

```
Router# show mpls interfaces interfaces
Router# show mpls cos-map cos-map
Router# show mpls prefix-map
```

Configuration Examples

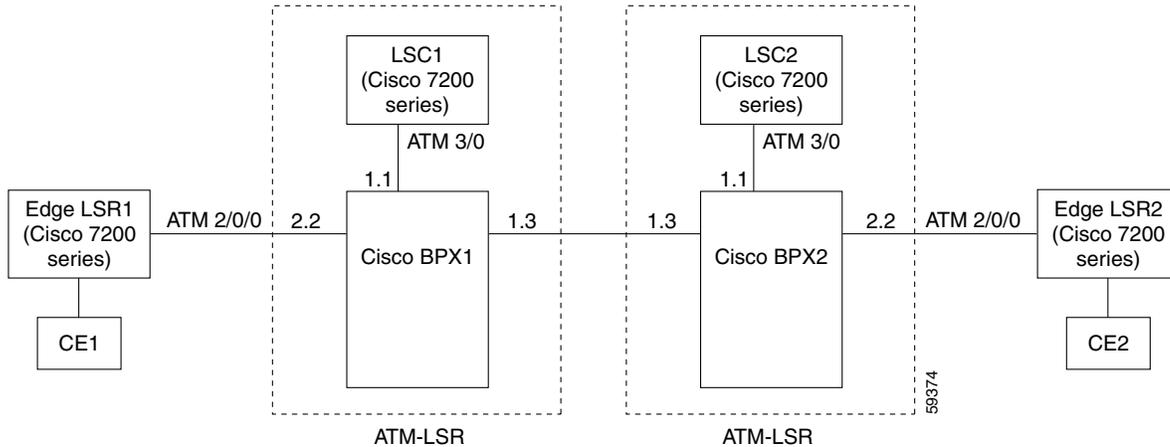
This section provides examples for the following configurations, based on the sample ATM LSR network configuration shown in [Figure 30](#):

- Configuration for a customer edge router (CE1)
- Configuration for LSC1
- Configuration for BPX1 and BPX2
- Configuration for LSC2
- Configuration for Edge LSR1
- Configuration for Edge LSR2

**Note**

The IGX series ATM switches do not support class of service (CoS).

Figure 30 Sample ATM LSR Network Configuration (CE1 to be added with connection to Edge LSR1)



Configuration for CE1

2600 or 3600 CE1:

```
interface Loopback0
  ip address 7.7.7.7 255.255.255.0
!
interface FastEthernet0/1
  ip address 150.150.0.2 255.255.255.0
  duplex auto
  speed auto
!
router ospf 1
  network 7.7.7.7 0.0.0.0 area 0
  network 150.150.0.0 0.0.0.255 area 0
```

Configuration for Edge LSR1

8850 with RPM-PR LSR1:

```
ip cef distributed
!
class-map match-all exp0
  match mpls experimental 0 4
class-map match-all exp1
  match mpls experimental 1 5
class-map match-all exp2
  match mpls experimental 2 6
class-map match-all exp3
  match mpls experimental 3 7
class-map match-all acl101
  match access-group 101
class-map match-all acl102
  match access-group 102
!
policy-map atm_output
  class exp0
    bandwidth percent 10
  class exp1
    bandwidth percent 25
  class exp2
    bandwidth percent 20
```

```

        class exp3
        bandwidth percent 20
    !
    policy-map input_int
        class acl101
            police cir 64000 bc 2000 conform-action set-mpls-exp-transmit 2 exceed-action
            set-mpls-exp-transmit 1
        class acl102
            police cir 32000 bc 1500 conform-action set-mpls-exp-transmit 3 exceed-action drop
    !
    interface loopback 0
        ip address 142.6.132.2 255.255.255.255
    !
    interface Ethernet1/1
        ip address 150.150.0.1 255.255.255.0
        service-policy input input_int
    !
    interface ATM2/0/0
        no ip address
    !
    interface ATM2/0/0.5 mpls
        ip unnumbered loopback 0
        service-policy output atm_output
        mpls atm vpi 2-5
        mpls atm multi-vc
        mpls ip
    !
    access-list 101 permit ip host 7.7.7.7 any
    access-list 102 permit ip host 150.150.0.2 any

```

Configuration for LSC1

7200 or 8850 with PRM-PR LSC1:

```

ip cef
!
interface loopback0
    ip address 192.103.210.5 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
    ip unnumbered loopback 0
    extended-port ATM3/0 bpx 1.3
    mpls atm vpi 2-15
    mpls atm cos available 20
    mpls atm cos standard 30
    mpls atm cos premium 25
    mpls atm cos control 25
    mpls ip
!
interface XTagATM23
    ip unnumbered loopback 0
    extended-port ATM3/0 bpx 2.2
    mpls atm vpi 2-5
    mpls atm cos available 20
    mpls atm cos standard 30
    mpls atm cos premium 25
    mpls atm cos control 25

```

```
mpls ip
```

Configuration for BPX1 and BPX2

BPX1 and BPX2:

```
uptrk 1.1
addshelf 1.1 v 1 1
cnfrsrc 1.1 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 1.3
cnfrsrc 1.3 256 252207 y 1 e 512 6144 2 15 26000 100000
uptrk 2.2
cnfrsrc 2.2 256 252207 y 1 e 512 4096 2 5 26000 100000
```

Configuration for LSC2

7200 or 8850 with RPM-PR LSC2:

```
ip cef
!
interface loopback0
 ip address 142.2.143.22 255.255.255.255
!
interface ATM3/0
no ip address
tag-control-protocol vsi
ip route-cache cef
!
interface XTagATM13
ip unnumbered loopback 0
 extended-port ATM3/0 bpx 1.3
 mpls atm vpi 2-15
 mpls atm cos available 20
 mpls atm cos standard 30
 mpls atm cos premium 25
 mpls atm cos control 25
 mpls ip
!
interface XTagATM23
 ip unnumbered loopback 0
 extended-port ATM3/0 bpx 2.2
 mpls atm vpi 2-5
 mpls atm cos available 20
 mpls atm cos standard 30
 mpls atm cos premium 25
 mpls atm cos control 25
 mpls ip
```

Configuration for Edge LSR2

7200 or 8850 with RPM-PR LSR2:

```
ip cef
!
class-map match-all exp0
 match mpls experimental 0 4
class-map match-all exp1
 match mpls experimental 1 5
class-map match-all exp2
 match mpls experimental 2 6
class-map match-all exp3
 match mpls experimental 3 7
class-map match-all acl101
```

```

    match access-group 101
class-map match-all acl102
    match access-group 102
!
policy-map atm_output
    class exp0
        bandwidth percent 10
    class exp1
        bandwidth percent 25
    class exp2
        bandwidth percent 20
    class exp3
        bandwidth percent 20
!
policy-map input_int
    class acl101
        police cir 64000 bc 2000 conform-action set-mpls-exp-transmit 2 exceed-action
        set-mpls-exp-transmit 1
    class acl102
        police cir 32000 bc 1500 conform-action set-mpls-exp-transmit 3 exceed-action drop
!
interface loopback 0
    ip address 142.2.142.2 255.255.255.255
!
interface Ethernet1/1
    ip address 160.160.0.1 255.255.255.0
    service-policy input input_int
!
interface ATM2/0
    no ip address
!
interface ATM2/0.9 mpls
    ip unnumbered loopback 0
    service-policy output atm_output
    mpls atm vpi 2-5
    mpls atm multi-vc
    mpls ip
!
access-list 101 permit ip host 8.8.8.8 any
access-list 102 permit ip host 160.160.0.1 any

```

Configuration for CE2

2600 or 3600 CE2:

```

interface Loopback0
    ip address 8.8.8.8 255.255.255.0
!
interface FastEthernet0/1
    ip address 160.160.0.1 255.255.255.0
    duplex auto
    speed auto
!
router ospf 1
    network 8.8.8.8 0.0.0.0 area 0
    network 160.160.0.0 0.0.0.255 area 0

```

QoS Support

If LSC1 supports QoS, but LSC2 does not, LSC1 makes VC requests for the following default classes:

- Control = CoS3
- Standard = CoS1

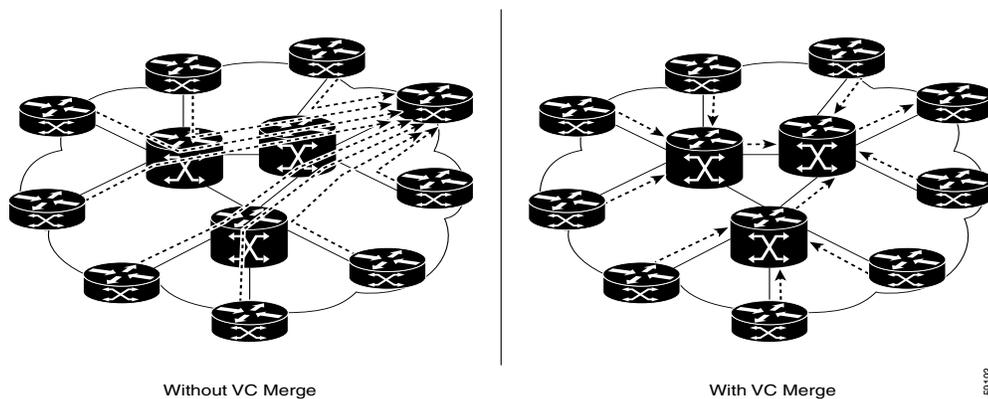
LSC2 ignores the call field in the request and allocates two UBR label VCs.

If LSR1 supports QoS, but LSR2 does not, LSR2 receives the request to create multiple label VCs, but by default, creates class 0 only (UBR).

Feature 5: MPLS VC Merge

The VC merge feature allows multiple incoming VCs to be merged into a single outgoing VC. This feature is only available on hardware that supports VC Merge functionality. See [VC Merge Hardware and Software Requirements](#) for more information. VC Merge helps scale MPLS networks, because it allocates only one VC to each destination on a link. [Figure 31](#) shows how VC merge streamlines the flow of frames in a network.

Figure 31 How VC Merge Improves the Flow of Information



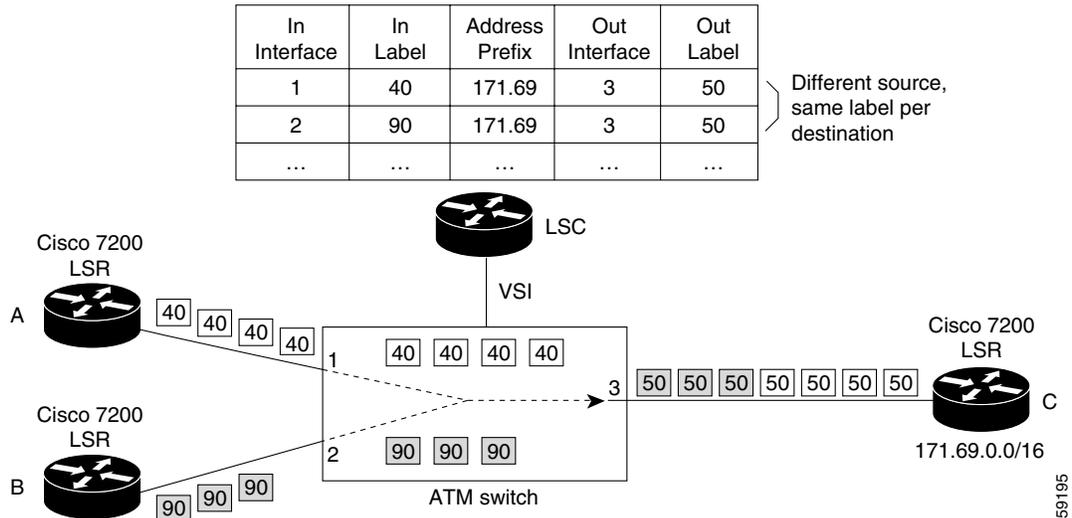
Feature Overview

VC merge maps several incoming labels to one single outgoing label. Cells from different virtual channel identifiers (VCIs) traveling to the same destination are transmitted to the same outgoing VC using multipoint-to-point connections.

VC merge allows the switch to transmit cells coming from different VCIs over the same outgoing VCI to the same destination. In other words, VC merge queues AAL5 frames in input buffers until the switch receives the last frame. Then the switch transmits the cells from that AAL5 frame before it sends any cells from other frames. VC merge requires the switch to provide buffering, but no more buffering than is required in IP networks. VC merge slightly delays the transfer of frames; however, VC merge is for IP traffic and not for traffic that requires speed. IP traffic tolerates delays better than other traffic on the ATM network.

In [Figure 32](#), routers A and B send traffic to router C (prefix 171.69.0.0/16). The ATM switch in the middle is configured with a single outbound VCI 50, which is bound to prefix 171.69.0.0/16. Data that flows from routers A and B congregates in the ATM switch and shares the same outgoing VC. The ATM switch buffers the cells from VCIs 40 and 90 until it receives all the AAL5 frames. Then, the switch forwards the complete frame router C on VCI 50.

Figure 32 How VC Merge Works



VC merge is enabled by default. To disable VC merge, enter the **no mpls ldp atm vc-merge** command in global configuration mode.

VC Merge Benefits

The VC merge feature makes MPLS networks highly scalable. Without VC merge, an IGX 8400 network can scale to about 22-64 Edge LSRs. The VC merge feature can expand the number of Edge LSRs 2 to 10 times that amount.



Note

This example is approximate. The following dependencies and assumptions change the scalability: port speed, number of ports used, enabling multi-VC QoS, reserving all LVCs for MPLS.

This sharing of labels reduces the total number of virtual circuits required for label switching. Without VC merge, each source-destination prefix pair consumes one label VC on each interface along the path. VC merge reduces the label space shortage by sharing labels for different flows with the same destination.

VC Merge Restrictions

- This feature is only available on hardware that supports VC Merge functionality. See [VC Merge Hardware and Software Requirements](#) for more information.

- If the LSC hardware does not support the VC merge feature, and you enter the **mpls ldp atm vc-merge** command, you receive a warning message. The LSC sets up point-to-point VCs.
- VC merge is not supported on subinterfaces.
- All switches in the same network must run the same versions of software and firmware.
- When VC merge is disabled, all existing LVCs are cleared. New LVCs are created, but their format is point to point. Likewise, when VC merge goes from a disabled state to an enabled state, all LVCs are cleared. New LVCs are created with a multipoint-to-point format.

VC Merge Hardware and Software Requirements

You need the following hardware, software, and firmware to enable the VC merge feature.

Hardware:

Cisco IGX 8400 switches with a UXM-E card

Cisco BPX 8600 series switches with a BXM-E card

Cisco MGX 8850 switches with an AXSM or AXSM-E card

Cisco IGX and BPX Switch Software

Release 9.3.10 or higher

IOS Software

12.2(8)T or higher

Related VC Merge Docs

[Designing MPLS for ATM: Dimensioning MPLS Label VC Space](#)

Configuration

The VC merge feature is enabled by default on devices that support the feature. To disable the VC merge feature, use the **no mpls ldp atm vc-merge** command.

Feature 6: MPLS Diff-Serv-Aware Traffic Engineering over ATM

Multiprotocol Label Switching Traffic Engineering (MPLS TE) supports the Diff-Serv-aware over ATM feature. MPLS TE allows constraint-based routing of IP traffic. One of the constraints satisfied by constraint-based routing is the availability of required bandwidth over a selected path. Diff-Serv-aware Traffic Engineering (DS-TE) extends MPLS traffic engineering to enable you to perform constraint-based routing of “guaranteed” traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by constraint-based routing for regular traffic. The more restrictive bandwidth is termed a sub-pool, while the regular TE tunnel bandwidth is called the global pool. (The sub-pool is a portion of the global pool.) Tunnels using the sub-pool bandwidth can be used in conjunction with MPLS quality of service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network. The ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher QoS performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

Guaranteed Bandwidth Service Configuration

You can configure two bandwidth pools for tunnel head-end, mid-point, and tail-end devices. (See [MPLS Diff-Serv-aware Traffic Engineering \(DS-TE\) over ATM](#) for configuration information.) Once these pools are configured, you can:

- Use one pool, the sub-pool, for tunnels that carry traffic requiring strict bandwidth guarantees or delay guarantees.
- Use the other pool, the global pool, for tunnels that carry traffic requiring only Differentiated Service.

Having a separate pool for traffic requiring strict guarantees allows you to limit the amount of such traffic admitted on any given link. Often, you can achieve strict QoS guarantees only if the amount of guaranteed traffic is limited to a portion of the total link bandwidth.

Having a separate pool for other traffic (best-effort or Diff-Serv traffic) allows you to have a separate limit for the amount of such traffic admitted on any given link. This is useful because it allows you to fill up links with best-effort or Diff-Serv traffic, thereby achieving a greater utilization of those links.

Providing Strict QoS Guarantees Using DS-TE Sub-pool Tunnels

A tunnel using sub-pool bandwidth can satisfy the stricter requirements if you do all of the following:

1. Select a queue—or in Diff-Serv terminology, select a PHB (per-hop behavior)—to be used exclusively by the strict guarantee traffic. Call this the “GB queue.”

For delay/jitter guarantees, use the Diff-Serv Expedited Forwarding PHB (EF PHB). On the Cisco 7200 it is the “priority” queue. You must configure the bandwidth of the queue to be at least equal to the bandwidth of the sub-pool.

For bandwidth guarantees, use the Diff-Serv Assured Forwarding PHB (AF PHB). On the Cisco 7200 you use one of the existing class-based weighted fair queuing (CBWFQ) queues.

2. Ensure that the guaranteed traffic sent through the sub-pool tunnel is placed in the GB queue *at the outbound interface of every tunnel hop*, and that no other traffic is placed in this queue.

You do this by marking the traffic that enters the tunnel with a unique value in the `mpls exp bits` field, and steering only traffic with that marking into the GB queue.

3. Ensure that this GB queue is never oversubscribed; that is, no more traffic is sent into the sub-pool tunnel than the GB queue can handle.

You do this by rate-limiting the guaranteed traffic before it enters the sub-pool tunnel. The aggregate rate of all traffic entering the sub-pool tunnel should be less than or equal to the bandwidth capacity of the sub-pool tunnel. Excess traffic can be dropped (for delay/jitter guarantees) or can be marked differently for preferential discard (for bandwidth guarantees).

4. Ensure that the amount of traffic entering the GB queue is limited to an appropriate percentage of the total bandwidth of the corresponding outbound link. The exact percentage to use depends on several factors that can contribute to accumulated delay in your network: your QoS performance objective, the total number of tunnel hops, the amount of link fan-in along the tunnel path, burstiness of the input traffic, and so on.

You do this by setting the sub-pool bandwidth of each outbound link to the appropriate percentage of the total link bandwidth (that is, by adjusting the `subpool kbps` parameter of the `ip rsvp bandwidth` command).

Providing Differentiated Service Using DS-TE Global Pool Tunnels

You can configure a tunnel using global pool bandwidth to carry best-effort as well as several other classes of traffic. Traffic from each class can receive differentiated service if you do all of the following:

1. Select a separate queue (a distinct Diff-Serv PHB) for each traffic class. For example, if there are three classes (gold, silver, and bronze) there must be three queues (Diff-Serv AF2, AF3, and AF4).
2. Mark each class of traffic using a unique value in the MPLS experimental bits field (for example gold = 4, silver = 5, bronze = 6).
3. Ensure that packets marked as Gold are placed in the gold queue, Silver in the silver queue, and so on. The tunnel bandwidth is set based on the expected aggregate traffic across all classes of service.

To control the amount of Diff-Serv tunnel traffic you intend to support on a given link, adjust the size of the global pool on that link.

Providing Strict Guarantees and Differentiated Service in the Same Network

Because DS-TE allows simultaneous constraint-based routing of sub-pool and global pool tunnels, strict guarantees and Diff-Serv can be supported simultaneously in a given network.

For More Information about MPLS Diff-Serv-aware over ATM

For more information on the MPLS Diff-Serv-aware over ATM feature and its configuration, see the following document:

[MPLS Diff-Serv-aware Traffic Engineering \(DS-TE\) over ATM](#)

Feature 7: MPLS: OAM Insertion and Loop Detection on LC-ATM

This feature allows you to use ATM OAM cells to detect a failure between cell-mode MPLS interfaces. If two Cisco routers are connected using an LC-ATM link or a logical link (VP tunnel interface), OAM cells are inserted at regular intervals and looped back on the remote end. When one side of the link goes down or if the logical link fails, the OAM cells cannot reach their destination, causing the interface to change to the down state. OAM management allows the status of LC-ATM interfaces to be identified. Using OAM management reduces the amount of time required to accurately reflect the status of the link.

Without OAM management, when one side of an LC-ATM link breaks, the other side of the link cannot detect the failure. The interface and the line protocol of the broken link are still in the up state.

You can configure the OAM management parameters and tune them to your network needs.

OAM management is enabled by default. If one Cisco router does not have same release of software (and thus does not have OAM management), the other router that has OAM management can detect the broken link.

This feature allows you to configure OAM management on the following types of interfaces:

- MPLS subinterfaces (interface atm $x/x.x$ mpls)
- Switch subinterfaces on route processor modules (RPMs) (interface switch 1. x mpls)
- Extended tag-switching interfaces on label switch controllers (interface xtagatm xx)

Prerequisites for MPLS: OAM Insertion and Loop Detection on LC-ATM

This feature has the following prerequisites:

- The device must support cell mode MPLS LC-ATM interfaces.

Restrictions for MPLS: OAM Insertion and Loop Detection on LC-ATM

This feature has the following restrictions:

- This feature works with ATM port adapters that support OAM cells.
- The control virtual circuit (VC) information is not displayed in the saved configuration if you use the default control VC and default LC-ATM OAM parameters
- If the control VC is not set to the default VPI or VCI values or any of the OAM parameters are not set to the default values, the control VC information is displayed in the saved configuration.

How to Configure MPLS: OAM Insertion and Loop Detection on LC-ATM



Note

If you use the default control VC and do not want to change the OAM defaults, you do not need to configure the interface for OAM management.

This procedure explains how to configure OAM management on the interface. You can also use this procedure to configure OAM management on an MPLS ATM or switch subinterface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface xtagatm**{*if-number*}
4. **mpls atm control-vc** *vpi vci*
5. **oam-pvc manage** [*seconds*]
6. **oam retry** [*up-count down-count retry-frequency*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface xtagatm { <i>if-number</i> } Example: Router(config)# interface xtagatm61	Specifies the XtagATM interface.
Step 4	mpls atm control-vc <i>vpi vci</i> Example: Router(config-subif)# mpls atm control-vc 0 32	Configures the control VC VPI and VCI values for the link to the MPLS peer. This command also enables you to enter control-VC configuration mode.

	Command or Action	Purpose
Step 5	oam-pvc manage [<i>seconds</i>] Example: Router(cfg-mpls-atm-cvc)# oam-pvc manage 25	(Optional) Specifies how often OAM cells should be sent. See the oam-pvc command for the default values.
Step 6	oam retry [<i>up-count down-count retry-frequency</i>] Example: Router(cfg-mpls-atm-cvc)# oam retry 2 3 4	(Optional) Specifies the OAM retry count before declaring a VC is up or down, and its polling frequency. See the oam retry command for the default values.

Troubleshooting Tips

Use the following commands to help troubleshoot:

- **show atm vc detail**
- **debug atm oam**

Configuration Examples for MPLS: OAM Insertion and Loop Detection on LC-ATM

This section provides the following configuration examples:

- [OAM Management with MPLS Subinterfaces Example, page 113](#)
- [OAM Management with Switch Subinterfaces on Route Processor Modules Example, page 113](#)
- [OAM Management with XtagATM Subinterfaces on Label Switch Controllers Example, page 114](#)

OAM Management with MPLS Subinterfaces Example

The following example show how to configure OAM management on an MPLS subinterface.

```
interface ATM3/0.100 mpls
 ip unnumbered Loopback0
 mpls atm control-vc 0 32
 oam-pvc manage 1
 mpls ip
```

OAM Management with Switch Subinterfaces on Route Processor Modules Example

The following example shows how to configure OAM management on a switch subinterface on an route processor module.

```
interface Switch1.10 mpls
 ip unnumbered Loopback0
 mpls atm control-vc 0 32
 oam retry 1 5 1
 oam-pvc manage 2
 mpls ip
```

OAM Management with XtagATM Subinterfaces on Label Switch Controllers Example

The following example shows how to configure OAM management on an XtagATM subinterface.

```
interface xtagatm113
  ip unnumbered Loopback0
  extended-port Switch1 descriptor "11:1.3:3"
  mpls atm control-vc 0 32
    oam retry 1 5 1
  mpls ip
```

Feature 8: Troubleshooting the MPLS LSC Network with the LVC Path Trace Feature

This section describes the LVC Path Trace feature, which enables you to display the path of an established LVC. The **show mpls atm-ldp bindings** command has been updated with the **path** keyword. By displaying the path of an LVC, it is easier to troubleshoot outages in an MPLS LSC network.

Prerequisites for the LVC Path Trace Feature

Before issuing the **show mpls atm-ldp bindings** command with the **path** keyword, ensure that LDP loop detection is enabled throughout the LC-ATM network. The LDP loop detection mechanism is used with the Downstream on Demand (DoD) method of label distribution, supplementing the DoD hop count mechanism to detect looping label switched paths (LSPs) that might occur during transient routing events. You enable LDP loop detection with the **mpls ldp loop-detection** global configuration command.

If LDP loop detection is not enabled, the following error message is displayed when you issue the **show mpls atm-ldp bindings** command with the **path** keyword:

```
%Cannot trace the path of LVCs, because LDP loop detection is not enabled for this LDP session
```

Ensure that LDP loop detection is configured before LDP sessions are configured. Issuing the **mpls ldp loop-detection** command on already existing LDP sessions has no effect. The following error message is displayed:

```
%Enabling loop detection has no effect on existing LDP sessions.
```

To determine if loop detection is enabled on DoD LDP sessions, you can issue the **show mpls ldp neighbor detail** command. In the following example, the last two lines of output show that LDP loop detection is on and the path vector limit of the LDP session is 20/20. (The path vector limit is configured with the **mpls ldp maxhops** command.)

```
Router# show mpls ldp neighbor detail

Peer LDP Ident: 10.0.3.42:1; Local LDP Ident 10.0.2.102:1
TCP connection: 10.0.3.42.11028 - 10.0.2.102.646
State: Oper; Msgs sent/rcvd: 46/46; Downstream on demand
Up time: 00:33:38; UID: 1; Peer Id 0;
LDP discovery sources:
Switch1.1; Src IP addr: 10.0.3.42
holdtime: 15000 ms, hello interval: 5000 ms
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
Clients: TC ATM
Loop Detection Peer/Local: on/on
Path vector Limit Peer/Local: 20/20
```

Restriction for the LVC Path Trace Feature

The LVC Path Trace feature cannot completely trace the path of an LVC if VC merge capability is enabled. If VC Merge is enabled on some nodes, **show mpls atm-ldp bindings** command with the **path** keyword displays the path only up to the merging point.

Tracing the Path of an LVC

When you issue the **show mpls atm-ldp bindings** command with the **path** keyword, the command displays the path of the LVC, from the source to its destination. The asterisk (*) next to the prefix indicates the address from where the command was issued. The path output is limited to four router IDs per line. If more than four routers exist in the path, the command output wraps to the next line. For more information about the command output, see the **show mpls atm-ldp bindings** command with the **path** keyword. The following example is a sample LVC path trace:

```
Router# show mpls atm-ldp bindings 10.0.2.115 32 path

Destination: 10.0.2.115/32
  Headend Router Switch1.1 (2 hops) 0/39 Active, VCD=9, CoS=available
    Path: 10.0.2.102* 10.0.3.42 10.0.2.115
  Headend Router Switch1.1 (2 hops) 0/41 Active, VCD=8, CoS=premium
    Path: 10.0.2.102* 10.0.3.42 10.0.2.115
  Headend Router Switch1.1 (2 hops) 0/43 Active, VCD=7, CoS=control
    Path: 10.0.2.102* 10.0.3.42 10.0.2.115
```

The path is always displayed from headend to tailend. If you display the path of a transit node, the prefix with the asterisk appears in the middle of the output. If you display the path of a tailend device, the prefix with the asterisk is at the end.

The following example shows the path of a transit node:

```
Destination: 10.0.0.13/32
  Headend Switch XTagATM1301 (1 hop) 0/87 Active, VCD=604, CoS=available
    Path: 10.0.0.10* 10.0.0.13
  Transit XTagATM4010202 0/3538 Active -> XTagATM1301 0/417 Active, CoS=available
    Path: 10.0.0.2 10.0.0.10* 10.0.0.13
  Transit XTagATM4010202 0/3594 Active -> XTagATM1301 0/477 Active, CoS=available
    Path: 10.0.0.11 10.0.0.2 10.0.0.10* 10.0.0.13
  Transit XTagATM10010202 0/2042 Active -> XTagATM1301 0/523 Active, CoS=available
    Path: 10.0.0.100 10.0.0.10* 10.0.0.13
  Transit XTagATM4010505 1/262 Active -> XTagATM1301 0/717 Active, CoS=available
    Path: 10.0.0.72 10.0.0.10* 10.0.0.13
  Transit XTagATM4010505 1/264 Active -> XTagATM1301 0/719 Active, CoS=standard
    Path: 10.0.0.72 10.0.0.10* 10.0.0.13
  Transit XTagATM4010505 1/266 Active -> XTagATM1301 0/721 Active, CoS=premium
    Path: 10.0.0.72 10.0.0.10* 10.0.0.13
  Transit XTagATM4010505 1/268 Active -> XTagATM1301 0/723 Active, CoS=control
    Path: 10.0.0.72 10.0.0.10* 10.0.0.13
```

The following example shows the path of a tailend device:

```
Destination: 10.0.2.142/32
  Tailend Router Switch1.1 0/5464 Active, VCD=10432, CoS=available
    Path: 10.0.2.112 10.0.3.25 10.0.2.142*
  Tailend Router Switch1.1 0/5466 Active, VCD=10433, CoS=premium
    Path: 10.0.2.112 10.0.3.25 10.0.2.142*
  Tailend Router Switch1.1 0/5468 Active, VCD=10434, CoS=control
    Path: 10.0.2.112 10.0.3.25 10.0.2.142*
  Tailend Router Switch1.1 0/8110 Active, VCD=11759, CoS=available
    Path: 10.0.2.92 10.0.3.42 10.0.3.25 10.0.2.142*
  Tailend Router Switch1.1 0/8112 Active, VCD=11760, CoS=premium
    Path: 10.0.2.92 10.0.3.42 10.0.3.25 10.0.2.142*
  Tailend Router Switch1.1 0/8114 Active, VCD=11761, CoS=control
    Path: 10.0.2.92 10.0.3.42 10.0.3.25 10.0.2.142*
```

Starting Up the Cisco MGX 8850 PXM-45 and Cisco MGX AXSM

The Cisco MGX 8850 AXSM Broadband ATM Switching Module is a high-density, high-speed module used in the Cisco MGX 8850 combined with the high-capacity PXM-45 processor switching module to deliver connectivity from T3/E3 to OC-48c/STM-16.

This section contains the following topics:

- [Before Startup, page 117](#)
- [Copying the Images from the TFTP Server, page 119](#)
- [Upgrading the PXM-45 and AXSM Images, page 122](#)
- [Verifying the IOS Files on the PXM-45 E:Drive, page 125](#)

Before Startup

This section contains information about the following:

- [Access Privileges, page 117](#)
- [Booting Order and Cautions, page 117](#)
- [File and Directory Names Are Case Sensitive, page 118](#)
- [Flash Command vs. Bootflash Command, page 118](#)
- [Upgrade Cisco MGX 8850 PXM-45 Card First, page 118](#)
- [Set Boot IP Address in Every Switch, page 118](#)
- [Image File Formats, page 118](#)

Access Privileges

The default username and password for access to the switch is **cisco**. In this mode, a limited set of commands are available for troubleshooting. If you log in during stage 1 and the card progresses to the “active” or “standby” state, the card logs out the stage 1 user and prompts you to log in again. At this point, you must log in as a user with configuration privileges and the corresponding password. The stage 1 username and password are not supported on active and standby cards.

To perform some startup procedures, you need to log in as a user with SUPER_GP privileges (default username and password: superuser, superuser).

To display detailed command lists, you must establish a session using a username with SERVICE_GP privileges or higher.

For more information on access privileges on the Cisco MGX 8850 switch, see the *Cisco MGX 8850 Routing Switch Command Reference, Release 2.1*.

Booting Order and Cautions

Make sure that you boot the Cisco 8850 PXM-45 Processor Switch Module properly with the correct PXM image. If the PXM-45 is not fully booted properly, you cannot reach any cards in the Cisco 8850 MGX switch. With a proper boot, you should get the “unknown.7.PXM.a>” prompt, or if you have already given the card a name, you should get a “name.7.PXM.a>” prompt. With either prompt, you can reach other cards.

The PXM-45 needs to be booted before you bring up the Cisco MGX 8850 RPM-PRs. Make sure that all RPM-PRs are booted properly with the correct image. Otherwise, the PXM does not recognize the RPM-PRs.

File and Directory Names Are Case Sensitive

You must use a capital E when referencing the E: drive in switch commands. File and directory names in the switch file system are case sensitive.

Flash Command vs. Bootflash Command

Although you can display directory contents with the **dir bootflash:** command, the **show flash:** command provides more detail. The terms *bootflash* and *flash* refer to the same entity on the RPM-PR; on other Cisco routers, bootflash and flash are separate entities.

Upgrade Cisco MGX 8850 PXM-45 Card First

Pay attention to the following if you plan to upgrade PXM-45 and AXSM cards:

- Upgrade the PXM-45 cards first. Wait until the PXM-45 cards are operating in active and standby modes with the correct software before upgrading AXSM cards.
- The software version used by the PXM-45/B cards should be equal to or later than the version used on the AXSM, AXSM/B, and AXSM-E cards.
- Upgrade the AXSM boot software before you upgrade the run-time software.
- If you are upgrading software on more than one AXSM card in the switch at the same time, wait until one AXSM card upgrade is complete before starting the upgrade on another AXSM card.

Set Boot IP Address in Every Switch

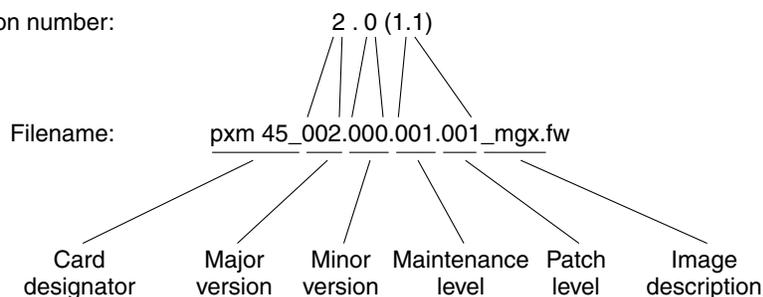
Because the LAN IP address is stored on the PXM-45 hard disk and is not used until after the run-time software loads, Cisco recommends that the boot IP address be set in every switch. This enables switch management over Ethernet when the boot software has loaded.

Image File Formats

Figure 33 illustrates the filename format for released software.

Figure 33 **Filename Format for Release Software**

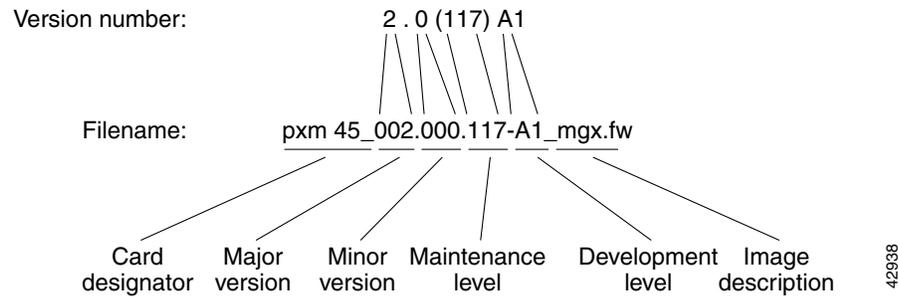
Version number:



42937

Figure 34 illustrates the filename format for prereleased firmware.

Figure 34 **Filename Format for Prereleased Software**



Copying the Images from the TFTP Server

To copy the software images for the Cisco MGX 8850 PXM-45 and Cisco MGX 8850 AXSM from the TFTP server to the Cisco MGX 8850 switch, perform the following steps:

- Step 1** On the PXM-45, set the node name for the switch using the **cnfname** command:

```
unknown.7.PXM.a > cnfname <node name>
```

Enter up to 32 characters for the *node name*. The Cisco MGX 8850 switch node name is case sensitive. Be sure to enter the name correctly. For example:

```
unknown.7.PXM.a > cnfname Switch
```

```
This node name will be changed to Switch. Please Confirm
cnfname: Do you want to proceed (Yes/No)? y
cnfname: Configured this node name to Switch Successfully.
SWITCH.7.PXM.a >
```

The new node name appears immediately in the next CLI prompt.

- Step 2** Verify the IP address of the Ethernet interface before you copy the image files from the TFTP server. Use the **dspipif interface** display command.



Note Make sure that you have a network connection from the PXM-45 card before trying to copy the image files.

For example:

```
SWITCH.7.PXM.a > dspipif lnPci0
SWITCH          System Rev: 02.01 Sep. 13, 2001 16:19:43 GMT
MGX8850         Node Alarm: MAJOR
IP INTERFACE CONFIGURATION
lnPci (unit number 0):
  Flags: (0x63) UP BROADCAST ARP RUNNING
  Internet address: 10.0.6.105
  Broadcast address: 0.255.255.255
  Netmask 0xff000000 Subnetmask 0xffff0000
  Ethernet address is 00:01:42:26:5f:b2
  Metric is 0
  Maximum Transfer Unit size is 1500
```

```

    20 packets received; 0 packets sent
    0 input errors; 0 output errors
    0 collisions
    DISK IP address: 10.0.6.105
SWITCH.7.PXM.a >

```

If the IP address is not configured, then you can configure the IP address, using the following command:

```

ipifconfig <interface> [ <ip_address> ] [ netmask <mask> ] [ broadcast <broad_addr> ]
[ up | down ] [ arp | noarp ] [ svc | nosvc ] [ pvc | nopvc ]
[ default | nodefault ] [ clrstats ]

```

Where:

- *<interface>* = the interface name—use **dspipif** to see valid values, for example, atm0, lnPci0, sl0
- *<ip_address>* = IP address for interface—*<ip_address>* has format a.b.c.d, for example, 172.29.21.96
- **netmask** *<mask>* = interface network mask—**netmask** is a keyword and *<mask>* has a format of a.b.c.d, for example, 255.255.0.0
- **broadcast** *<broad_addr>* = interface broadcast address—**broadcast** is a keyword and *<broad_addr>* has a format of a.b.c.d, for example, 172.29.255.255

For example:

```

SWITCH.7.PXM.a > ipifconfig lnPci0 10.0.6.105 netmask 255.255.0.0 up

```

You can verify the IP address of the Ethernet interface, using the **dspipif lnPci0** command.

- Step 3** Save the existing configuration with the **saveallcnf** command. This command saves the configuration to a file in the C:/CNF directory. The file is named using the switch name and the current date as follows: *Name_01_DateTime.zip*.

```

SWITCH.7.PXM.a > saveallcnf
The 'saveallcnf' command can be time-consuming. The shelf
must not provision new circuits while this command is running.

```

Do not run this command unless the shelf configuration is stable or you risk corrupting the saved configuration file.

```

Do you want to proceed (Yes/No)? y
saveallcnf: shelf configuration saved in C:/CNF/Switch_01_200109151550.zip.

```



Caution Avoid making configuration changes while upgrading PXM-45 software. Configuration changes can be lost when the PXM45 is reset during the upgrade.

- Step 4** Go to the directory where the images are located, **/tftpboot/mpls/atm_mpls/MGX/pxm_axsm_images**, and identify the PXM and AXSM images to be loaded in the Cisco MGX 8850 switch.

```

Workstation> ls

002.001.060.008-P2.tar          pxm1_001.001.060.008-P1_bt
002.001.060.008-P2.tar.txt     pxm1_001.001.060.008-P1_bt.fw
2.01.60.8-P2.catcs             pxm1_001.001.060.008-P1_bt.hex
CWM_UPGRD                      pxm1_001.001.060.008-P1_bt.map
axsm_002.001.060.008-A_bt      pxm1_001.001.060.008-P1_ses
axsm_002.001.060.008-A_bt.fw   pxm1_001.001.060.008-P1_ses.fw
axsm_002.001.060.008-A_bt.hex  pxm1_001.001.060.008-P1_ses.map
axsm_002.001.060.008-A_bt.map  pxm45_002.001.060.008-P1_bt
axsm_002.001.060.008-P2       pxm45_002.001.060.008-P1_bt.fw
axsm_002.001.060.008-P2.fw    pxm45_002.001.060.008-P1_bt.hex
axsm_002.001.060.008-P2.map    pxm45_002.001.060.008-P1_bt.map

```

```

axsme_002.001.060.008-A_bt      pxm45_002.001.060.008-P1_mgx
axsme_002.001.060.008-A_bt.fw  pxm45_002.001.060.008-P1_mgx.fw
axsme_002.001.060.008-A_bt.hex pxm45_002.001.060.008-P1_mgx.map
axsme_002.001.060.008-A_bt.map release.notes
axsme_002.001.060.008-P1      rpm-boot-mz.122-3.4.T
axsme_002.001.060.008-P1.fw   rpm-js-mz.122-3.4.T
axsme_002.001.060.008-P1.map

```

- Step 5** Copy the PXM-45 and the AXSM images from the TFTP server to the C:/FW directory on the Cisco MGX 8850 switch using the **ftp <destination-address>** command.



Note You cannot start the FTP process from the Cisco MGX 8850 switch.

```

Workstation> ftp 10.0.6.105
Connected to 10.0.6.105.
220 VxWorks FTP server (VxWorks 5.3.1) ready.
Name (10.0.6.105:username): cisco
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> cd FW
250 Changed directory to "C:FW"
ftp> put pxm45_002.001.060.008-P1_bt.fw
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
local: pxm45_002.001.060.008-P1_bt.fw remote: pxm45_002.001.060.008-P1_bt.fw
897616 bytes sent in 9.2 seconds (96 Kbytes/s)
Hash mark printing on (8192 bytes/hash mark).
ftp> put pxm45_002.001.060.008-P1_mgx.fw
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
local: pxm45_002.001.060.008-P1_mgx.fw remote: pxm45_002.001.060.008-P1_mgx.fw
4889196 bytes sent in 49 seconds (97 Kbytes/s)
ftp> put axsme_002.001.060.008-P2.fw
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
local: axsme_002.001.060.008-P2.fw remote: axsme_002.001.060.008-P2.fw
2651752 bytes sent in 27 seconds (97 Kbytes/s)
ftp> put axsme_002.001.060.008-A_bt.fw
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
local: axsme_002.001.060.008-A_bt.fw remote: axsme_002.001.060.008-A_bt.fw
634528 bytes sent in 6.5 seconds (96 Kbytes/s)
ftp> bye
221 Bye...see you later
Workstation>

```

- Step 6** Verify that the PXM-45 and AXSM images are in the C:/FW directory on the Cisco MGX 8850 switch. Your current directory is C. You first need to change the directory to C:/FW using the **cd** command.

```
SWITCH.7.PXM.a > cd FW
```

Then, you can list the files on this directory using the **ls** or **dir** command.

```
SWITCH.7.PXM.a > ls
```

```

..
pxm45_002.000.002.000_mgx.fw
pxm45_002.000.002.000_bt.fw
axsm_002.000.002.000.fw
axsm_002.000.002.000_bt.fw
pxm45_002.001.000.235-A_bt.fw
rpm-boot-mz_002.001.000.040
rpm-js-mz_002.001.000.040
axsm_002.001.000.040-A.fw
axsm_002.001.000.210-A_bt.fw
pxm45_002.001.000.040-P1_mgx.fw
pxm45_002.001.060.008-P1_bt.fw
pxm45_002.001.060.008-P1_mgx.fw
axsm_002.001.060.008-P2.fw
axsm_002.001.060.008-A_bt.fw
In the file system :
  total space : 819200 K bytes
  free space  : 755677 K bytes

```

The files copied from the server are highlighted in the example.



Note For more details on these procedures, refer to the Cisco MGX 8850 switch documentation for the current release.

Upgrading the PXM-45 and AXSM Images

To upgrade the software images for the Cisco MGX 8850 PXM-45 and Cisco MGX 8850 AXSM cards, perform the following steps:

Step 1 Change to the C directory on the PXM-45 card.



Note You need to be in the C directory to perform an upgrade on either a PXM-45 or AXSM card.

```

SWITCH.7.PXM.a > cd ..
SWITCH.7.PXM.a > sh

```

Wait until the display is complete before continuing to the next step.

Step 2 Enter the **sysBackupBoot** command. At the `pxm45bkup>` prompt burn the boot software on the PXM-45 using the **sysFlashBootBurn** *filename* command. Replace *filename* with the complete path to the boot file on the PXM-45 hard drive.

```

pxm45>sysBackupBoot
pxm45bkup> sysFlashBootBurn "C:FW/pxm45_002.001.060.008-P1_bt.fw"
Burning backup boot from file=C:FW/pxm45_002.001.060.008-P1_bt.fw
Please confirm:[y/n] y
ImgHdr: image_type=2,shelf_type=5,card_type=3000
Checksum size is 897616 ...
Simulating PXM Card removal.
Downloading C:FW/pxm45_002.001.060.008-P1_bt.fw into the flash ...
QUERY TABLE: flash_size=8388608 block_size=131072 write_buf_size=32
             buf_wr_time=2048 write_time=2048 erase_time=16384000
burning 0xbfc00000 verify ... ok
burning 0xbfc20000 verify ... ok

```

```

burning 0xbfc40000 verify ... ok
burning 0xbfc60000 verify ... ok
burning 0xbfc80000 verify ... ok
burning 0xbfca0000 verify ... ok
burning 0xbfcc0000 verify ... ok
Verify checksum: addr=0xbfc00000 chksum=0x91ce90e3 size=(0xdb250,897616)...ok
Flash download completed ...
value = 0 = 0x0
pxm45bkup>reboot
Login: Entering rvtAct...
BertCtcAppEventHandler
Attaching network interface sl0... done.
Login: Cisco
password:

```

Step 3 Verify that the boot software is on the PXM-45 hard drive using the **dspcd slot** command:

```

SWITCH.7.PXM.a > dspcd 7
SWITCH                               System Rev: 02.01 Sep. 13, 2001 16:48:18 GMT
MGX8850                               Node Alarm: MAJOR
Slot Number 7 Redundant Slot: 8
Front Card      Upper Card      Lower Card
-----
Inserted Card: PXM45                UI Stratum3      PXM HardDiskDrive
Reserved Card: PXM45                UI Stratum3      PXM HardDiskDrive
State:          Active-U           Active           Active
Serial Number:  SBK0447009D         SBK044200XM     SBK043600GV
Prim SW Rev:    2.1(0.40)P1         ---             ---
Sec SW Rev:    2.1(0.40)P1         ---             ---
Cur SW Rev:    2.1(0.40)P1         ---             ---
Boot FW Rev:   2.1(60.8)P1         ---             ---
800-level Rev: B0                   A0              A0
800-level Part#: 800-06147-07       800-05787-02   800-05052-04
CLEI Code:     BAA5KMZCAA           BA7IBCLAAA     BA7IADNAAA
Reset Reason:  On Power up
Card Alarm:    NONE
Failed Reason: None
Miscellaneous Information:
Type <CR> to continue, Q<CR> to stop: q

```

The new boot firmware is highlighted in the example.

Step 4 Load the image in the PXM-45 in slot using the **loadrev slot revision** command.



Note Loading the upgrade run-time software version on a PXM-45 or AXSM card uses the same **loadrev slot revision** command.

```

SWITCH.7.PXM.a > loadrev 7 2.1(60.8)P1
one or more card(s) in the logical slot may be reset.
loadrev: Do you want to proceed (Yes/No)? y

```

Step 5 Verify that the image was loaded into slot 7 in the PXM-45 using the **dspcd slot** command.

```

SWITCH.7.PXM.a > dspcd 7
SWITCH                               System Rev: 02.01 Sep. 13, 2001 18:24:20 GMT
MGX8850                               Node Alarm: MAJOR
Slot Number 7 Redundant Slot: 8
Front Card      Upper Card      Lower Card
-----
Inserted Card: PXM45                UI Stratum3      PXM HardDiskDrive
Reserved Card: PXM45                UI Stratum3      PXM HardDiskDrive

```

```

State:           Active-U           Active           Active
Serial Number:  SBK0447009D         SBK044200XM     SBK043600GV
Prim SW Rev:    2.1(0.40)P1         ---             ---
Sec SW Rev:    2.1(60.8)P1         ---             ---
Cur SW Rev:    2.1(0.40)P1         ---             ---
Boot FW Rev:   2.1(60.8)P1         ---             ---
800-level Rev:  B0                  A0              A0
800-level Part#: 800-06147-07      800-05787-02   800-05052-04
CLEI Code:      BAA5KMZCAA         BA7IBCLAAA     BA7IADNAAA
Reset Reason:   On Power up
Card Alarm:     NONE
Failed Reason:  None
Miscellaneous Information:
Type <CR> to continue, Q<CR> to stop: q

```

The new firmware and software images are highlighted in this example.

- Step 6** Start the new run-time software version on a PXM-45 (or on an AXSM card), by entering the **runrev slot revision** command.

```

SWITCH.7.PXM.a > runrev 7 2.1(60.8)P1
one or more card(s) in the logical slot may be reset.
runrev: Do you want to proceed (Yes/No)? y

```

- Step 7** Enter the **burnboot slot revision** command to burn the boot software on the standby AXSM card. You need to specify the slot number of the standby card, in this case slot 11.

```

SWITCH.7.PXM.a > burnboot 11 2.1(60.8)A
The card in slot 11 will be reset.
burnboot: Do you want to proceed (Yes/No)? y

```

- Step 8** Load the image in the AXSM in slot 11 using the **loadrev slot revision** command. Then start using the new run-time software version by entering the **runrev slot revision** command.

```

SWITCH.7.PXM.a > loadrev 11 2.1(60.8)A
one or more card(s) in the logical slot may be reset.
loadrev: Do you want to proceed (Yes/No)? y

```

```

SWITCH.7.PXM.a > runrev 11 2.1(60.8)P2
one or more card(s) in the logical slot may be reset.
runrev: Do you want to proceed (Yes/No)? y

```

The card goes through many states, but should settle in the **Active-U** state.

- Step 9** Verify that the AXSM image loaded properly using the **dspcd slot** command.



Note If you have multiple AXSM or other cards, make sure you have loaded the image properly on all the cards. Use the **dspcd slot** command to verify the image status.

```

SWITCH.7.PXM.a > dspcd 11
SWITCH                               System Rev: 02.01 Sep. 13, 2001 18:40:26 GMT
MGX8850                               Node Alarm: MAJOR
Slot Number: 11 Redundant Slot: NONE
          Front Card           Upper Card           Lower Card
          -----
Inserted Card: AXSM_160C3      MMF_8_OC3_MT        ---
Reserved Card: UnReserved     UnReserved           UnReserved
State:           Active-U           Active           Empty
Serial Number:  SBK044200H5         SBK044301MQ       ---
Prim SW Rev:    2.1(60.8)P2         ---               ---
Sec SW Rev:     ---                 ---               ---
Cur SW Rev:    2.1(60.8)P2         ---               ---

```

```

Boot FW Rev:      2.1(60.8)A      ---      ---
800-level Rev:
800-level Part#: 800-05776-06      800-04819-01      ---
CLEI Code:        BAA5HLXCAA      BAA5Z8UCAA      ---
Reset Reason:     On Power up
Card Alarm:       NONE
Failed Reason:    None
Miscellaneous Information:
Type <CR> to continue, Q<CR> to stop:
Switch           System Rev: 02.01 Sep. 13, 2001 18:40:26 GMT
MGX8850          Node Alarm: MAJOR
Crossbar Slot Status: Present
Alarm Causes
-----
NO ALARMS

```

**Note**

For more details on these procedures, refer to the Cisco MGX 8850 switch documentation for the current release.

Verifying the IOS Files on the PXM-45 E:Drive

The IOS image can be stored on the PXM-45 hard drive. To confirm this, make sure you are in the E:RPM directory and enter the **ll** command to list the contents of the directory. You should see a file named **rpm-js-mz_002.001.000.057**, or with a similar name beginning with rpm-js-mz, which is the IOS image.

**Tip**

Copy the RPM-PR Cisco IOS image into the RPM directory of the PXM-45 hard disk with the filename specified in the RPM-PR boot command.

The following screen displays the PXM E:RPM content listing:

```

SWITCH.7.PXM.a > cd E:RPM
SWITCH.7.PXM.a >

```

size	date	time	name
512	FEB-23-2001	17:59:54	.
512	FEB-23-2001	17:59:54	..
2452288	FEB-23-2001	11:13:10	rpm-boot-mz_002.001.000.057
7934768	FEB-23-2001	11:15:24	rpm-js-mz_002.001.000.057
744	FEB-27-2001	10:24:22	auto_config_slot11

```

In the file system :
total space : 102400 K bytes
free space : 91984 K bytes

```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls xtagatm cross-connect**
- **debug mpls xtagatm errors**
- **debug mpls xtagatm events**
- **debug mpls xtagatm vc**
- **debug vsi api**
- **debug vsi errors**
- **debug vsi events**
- **debug vsi packets**
- **debug vsi param-groups**
- **extended-port**
- **interface xtagatm**
- **mpls atm control-vc**
- **mpls atm cos**
- **mpls atm disable-headend-vc**
- **mpls ldp atm vc-merge**
- **mpls atm vpi**
- **mpls atm vp-tunnel**
- **mpls request-labels for**
- **oam-pvc**
- **oam retry**
- **show atm vc**
- **show controllers vsi control-interface**
- **show controllers vsi descriptor**
- **show controllers vsi session**
- **show controllers vsi status**
- **show controllers vsi traffic**
- **show controllers xtagatm**
- **show interface xtagatm**
- **show mpls atm-ldp bindings**
- **show mpls atm-ldp bindwait**
- **show mpls atm-ldp capability**
- **show mpls atm-ldp summary**

- **show xtagatm cos-bandwidth-allocation xtagatm**
- **show xtagatm cross-connect**
- **show xtagatm vc**
- **tag-control-protocol vsi**

Glossary

The terms in this glossary are defined in an MPLS context, rather than a general usage context.

AIP—ATM Interface Processor. An ATM interface for Cisco 7000 series routers designed to minimize performance bottlenecks at the user-network interface (UNI).

Alien Port Adapter—A dual-wide port adapter for the Cisco 7200 router. The Alien Port Adapter is ABR-ready and supports traffic shaping.

ATM Edge LSR—A router that is connected to the ATM-LSR cloud through LSC-ATM interfaces. The ATM Edge LSR adds labels to unlabeled packets and strips labels from labeled packets.

ATM Lite—Entry-level port adapter (higher performance than the AIP) for 7200 routers. The ATM Lite does not support traffic shaping or ABR.

ATM-LSR—A label switch router with several LSC-ATM interfaces. The router forwards the cells among these interfaces using labels carried in the VPI/VCI field of the cells.

BPX—Broadband Packet Exchange. A carrier-quality switch with trunk and CPU hot standby redundancy.

BXM—Broadband Switch Module. An ATM port card for the Cisco BPX switch.

CAR—committed access rate. CAR is the main feature supporting packet classification. CAR uses the type of service (ToS) bits in the IP header to classify packets. You can use the CAR classification commands to classify and reclassify a packet.

Controlled ATM Switch—An ATM switch that is controlled by an LSC.

CoS—class of service. A feature that provides scalable, differentiated types of service across an MPLS network.

downstream on demand—Indicates that the downstream-on-demand method of label distribution is being used for this LDP session. When the downstream-on-demand method is used, an LSR advertises its locally assigned (incoming) labels to its LDP peer device only when the peer device asks for them.

DWFQ—VIP-Distributed WFQ (weighted fair queuing).

DWRED—VIP-Distributed WRED (weighted random early detection).

extended label ATM interface—A type of interface supported by the remote ATM switch driver and a particular switch-specific driver that supports MPLS over an ATM interface on a remotely controlled switch.

external ATM interface—One of the interfaces on the controlled ATM switch other than the switch control port. It is also referred to as an exposed ATM interface, because it is available for connections outside of the label-controlled switch.

IP Precedence—A 3-bit value in the type of service (ToS) byte used for assigning precedence to IP packets.

label—A short fixed-length label that tells switching nodes how the data (packets or cells) should be forwarded.

label controlled switch—The label switch controller and the controlled ATM switch that it controls, viewed together as a unit.

label imposition—The act of putting the first label on a packet.

label switch—A node that forwards units of data (packets or cells) on the basis of labels.

LBR—label bit rate. Service category defined by this document for label-VC traffic. Link and per-VC bandwidth sharing may be controlled by relative bandwidth configuration at the edge and each switch along a label-VC. No ATM traffic-related parameters specified.

LC-ATM (label-controlled ATM) interface—An MPLS interface in which labels are carried in the VPI or VCI fields of the ATM cells and in which VC connections are established under the control of MPLS software.

LFIB—Label forwarding information base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

LSC—label switch controller. A Cisco IOS platform that runs the generic MPLS software and that can control the operation of an external ATM (or other type of) switch, making the interfaces of the latter appear externally as XtagATM interfaces.

LSP—label switched path. A configured connection between two routers, using MPLS to carry the packets.

LSR—label switching router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

LVC—label virtual circuit. A virtual circuit (VC) established under the control of MPLS. An LVC is neither a PVC nor an SVC. The LVC must traverse only a single hop in a label-switched path (LSP), but the LVC may traverse several ATM hops only if the LVC exists within a VP tunnel.

master control port—A physical interface on an MPLS LSC that is connected to one end of a slave control link.

MPLS—Multiprotocol Label Switching. An emerging industry standard on which label switching is based.

PNNI—Private Network-Network Interface.

PVC—permanent virtual circuit (or connection). A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection. Compare with SVC. See also virtual circuit.

PVP—permanent virtual path. A virtual path that consists of PVCs. See also PVC and virtual path.

QoS—quality of service. A measurement of performance for a transmission system that reflects its transmission quality and service availability.

RED—random early detection. Congestion avoidance algorithm in which a small percentage of packets are dropped when congestion is detected and before the queue in question overflows completely.

remote ATM switch driver—A set of interfaces that allows Cisco IOS software to control the operation of a remote ATM switch through a control protocol, such VSI.

ships in the night mode—The ability to support both MPLS functions and ATM forum protocols on the same physical interface, or on the same router or switch platform. In this mode, the two protocol stacks operate independently.

Switch control port—An interface that uses an MPLS LSC to control the operation of a controlled ATM switch (for example, VSI). The protocol runs on an ATM link.

SVC—switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. See also virtual circuit. Called a switched virtual connection in ATM terminology. Compare with PVC.

ToS—type of service. A byte in the IPv4 header.

VCC—virtual channel connection. Logical circuit, made up of VCLs, that carries data between two end points in an ATM network. Sometimes called a virtual circuit connection. See also VCL and VPI.

VCI—virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next network VCL that a cell needs to transit on its way to its final destination. The function of the VCI is similar to that of the DLCI in Frame Relay. Compare with DLCI.

VCL—virtual channel link. A connection between two ATM devices.

virtual circuit—Logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC). Virtual circuits are used in Frame Relay and X.25. In ATM, a virtual circuit is called a virtual channel. Sometimes abbreviated VC.

VNNI—Virtual Network-Network Interface.

VPC—virtual path connection. Grouping of VCCs that share one or more contiguous VPL. See also VCC and VPL.

VPI—virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next VCL that a cell needs to transit on its way to its final destination. The function of the VPI is similar to that of the DLCI in Frame Relay.

VPN—virtual private network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

VSI—Virtual Switch Interface. The protocol that enables an MPLS LSC to control an ATM switch over an ATM link.

VSI master—A VSI master process implementing the master side of the VSI protocol in a VSI controller. Sometimes the whole VSI controller is referred to as a “VSI Master;” but this is not strictly correct.

1. A device that controls a VSI switch, for example, a VSI Label Switch Controller.
2. A process implementing the master side of the VSI protocol.

VSI slave—A VSI slave is either of the following definitions:

1. A switch (in the “Single Slave model”) or a port card (in the “Multiple Slave Model”) that implements the VSI.
2. A process implementing the slave side of the VSI protocol.

WEPD—Weighted Early Packet Discard. A variant of EPD used by some ATM switches for discarding a complete AAL5 frame when a threshold condition, such as imminent congestion, is met. EPD prevents congestion that would otherwise jeopardize the ability of the switch to properly support existing connections with a guaranteed service.

WRED—weighted random early detection. A variant of RED in which the probability of a packet being dropped depends on its IP Precedence, CAR marking, or MPLS CoS (as well as other factors in the RED algorithm).

WFQ—weighted fair queuing. A queue management algorithm that provides a certain fraction of link bandwidth to each of several queues, based on relative bandwidth applied to each of the queues.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



MPLS Enhancements to Interfaces MIB

First Published: March 15, 2004

Last Updated: April 18, 2008

This document describes the Multiprotocol Label Switching (MPLS) enhancements to the existing Interfaces MIB (RFC 2233) to support an MPLS layer. This layer provides counters and statistics specifically for MPLS.

History for MPLS Enhancements to Interfaces MIB Feature

Release	Modification
12.0(23)S	This feature was introduced.
12.3(8)T	This feature was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This feature was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for MPLS Enhancements to Interfaces MIB, page 2](#)
- [Restrictions for MPLS Enhancements to Interfaces MIB, page 2](#)
- [Information About MPLS Enhancements to Interfaces MIB, page 3](#)
- [How to Configure MPLS Enhancements to Interfaces MIB, page 8](#)
- [Configuration Examples for the MPLS Enhancements to Interfaces MIB, page 10](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2004–2008 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 10](#)
- [Command Reference, page 12](#)
- [Glossary, page 13](#)

Prerequisites for MPLS Enhancements to Interfaces MIB

- SNMP must be installed and enabled on the label switching routers (LSRs)
- MPLS must be enabled on the LSRs
- MPLS IP must be enabled on an interface or an MPLS traffic engineering (TE) tunnel enabled on an interface

Restrictions for MPLS Enhancements to Interfaces MIB

- Link up and link down traps for the MPLS layer are not supported in this release.
- Write capability using the SNMP SET command is not supported for the MPLS layer in this release.
- Some counters, including discard and multicast, increment on the underlying physical layer; therefore, they equal 0 because they never reach the MPLS layer.
- Starting in Cisco IOS Release 12.4, the high-capacity counters for the MPLS layer interfaces of the Interfaces MIB contain 64 bits of counter data. In previous releases, the high capacity counters displayed 32 bits of counter data.

The following MIB objects are affected:

- ifHCInOctets
- ifHCOctets
- ifHCInUcastPkts
- ifHCOctetsUcastPkts

When the 64-bit values are less than the value of 232, the 32-bit and 64-bit values are identical.

After the counter increases to more than 232, the counters are different; the 64-bit value is computed by the following formula:

$$X * (232) + Y$$

where:

- X is the number of times the 32-bit counter has rolled.
- Y is the residual value of the counter after the roll occurred. The Y value equals the 32-bit value.

When the high-capacity counter values are compared to their 32-bit values, there is a period of time that the counter values are not equal. The 64-bit values lag the 32-bit values when the counters poll the 32-bit hardware counters and computing the correct counter value. During the polling and computation interval, the following high-capacity counter values counters might be inconsistent:

- ifInOctets
- ifOutOctets
- ifInUcastPkts
- ifOutUcastPkts

The inconsistent values can occur if traffic is constantly flowing over an interface and a MIB walk is performed. The 32-bit value is correct at that moment. The 64-bit value lags slightly, because of the polling computations needed to generate it. Once traffic stops flowing over the interface, and a polling period has passed, the two counters are identical and correct.

The lag time depends on the following factors:

- The polling interval used by the Interfaces MIB. The less time the polling interval takes, the more accurate the value is.
- The size of the Interfaces MIB. A large MIB takes a long time to walk and might affect the values found at that instant.
- The number of computations needed to generate the 64-bit value. The number of MPLS-enabled interfaces increases the number of 64-bit counter values that need to be computed.

Information About MPLS Enhancements to Interfaces MIB

To configure the MPLS Enhancements to Interfaces MIB, you need to understand the following concepts:

- [Feature Design of the MPLS Enhancements to Interfaces MIB, page 3](#)
- [Interfaces MIB Scalar Objects, page 5](#)
- [Stacking Relationships for MPLS Layer Interfaces, page 5](#)
- [Stacking Relationships for Traffic Engineering Tunnels, page 6](#)
- [MPLS Label Switching Router MIB Enhancements, page 7](#)
- [Benefits of the MPLS Enhancements to Interfaces MIB, page 8](#)

Feature Design of the MPLS Enhancements to Interfaces MIB

The Interfaces MIB (IF MIB) provides an SNMP-based method for managing interfaces. Each entry in the IF MIB establishes indexing, statistics, and stacking relationships among underlying physical interfaces, subinterfaces, and Layer 2 protocols that exist within Cisco IOS software.

The enhancements add an MPLS layer to the IF MIB as a Layer 2 protocol to provide statistics for traffic encapsulated as MPLS on an interface. In this structure, MPLS-specific data such as MPLS-encapsulated traffic counters and the MPLS maximum transmission unit (MTU) resides on top of the underlying physical or virtual interface to allow separation from non-MPLS data.

The enhancements also allow you to display indexing, statistics, and stacking relationships using the `ifStackTable`. MPLS layer interfaces are stacked above the underlying physical or virtual interface that is actually forwarding the MPLS traffic. MPLS traffic engineering tunnels are then stacked above those MPLS layers.

The IF MIB supports several types of interfaces. A virtual interface that provides protocol statistics for MPLS-encapsulated traffic has been added. This interface is stacked above real Cisco IOS interfaces or subinterfaces, such as Ethernet (et0) or ATM (at1/1.1).

Cisco IOS software creates a corresponding MPLS layer above each interface capable of supporting MPLS when the MPLS encapsulation is enabled by issuing the `mpls ip` interface configuration command.

You can also create the interface layer if you enable MPLS TE by using the **mpls traffic-eng tunnels** command in interface configuration mode.

**Note**

You must also issue these commands in global configuration mode for MPLS IP or MPLS TE to be enabled.

An IF MIB entry is created when you enable either MPLS IP or MPLS TE tunnels on an interface; the entry is removed when you disable both MPLS IP and MPLS TE.

ifStackTable Objects

Table 1 defines the ifStackTable objects.

Table 1 *ifStackTable Objects and Definitions*

Object	Definition
ifStackHigherLayer	The value of ifIndex corresponding to the higher sublayer of the relationship; that is, the sublayer that runs on top of the sublayer identified by the corresponding instance of the ifStackLowerLayer. Note Index objects are not accessible in a MIB walk. This value is part of the object identifier (OID) for every object in the ifStackTable.
ifStackLowerLayer	The value of ifIndex corresponding to the lower sublayer of the relationship; that is, the sublayer that runs below the sublayer identified by the corresponding instance of the ifStackHigherLayer. Note Index objects are not accessible in a MIB walk. This value is part of the OID for every object in the ifStackTable.
ifStackStatus	Used to create and delete rows in the ifStackTable; status is always active(1) for MPLS.

ifRcvAddressTable Objects

Table 2 defines the ifRcvAddressTable objects.

**Note**

Entries for the MPLS layer do not appear in the ifRcvAddressTable.

Table 2 *ifRcvAddressTable Objects and Descriptions*

Object	Definition
ifRcvAddressAddress	An address for which the system accepts packets and frames on this entry's interface. Note Index objects are not accessible in a MIB walk. This value is part of the OID for every object in the ifRcvAddressTable.
ifRcvAddressStatus	Used to create and delete rows in the ifRcvAddressTable.
ifRcvAddressType	Type of storage used for each entry in the ifRcvAddressTable.

Interfaces MIB Scalar Objects

The IF MIB supports the following scalar objects:

- **ifStackLastChange**—The value of sysUpTime at the time of the last change of the entire interface stack. A change of the interface stack is defined to be any creation, deletion, or change in value of any instance of ifStackStatus. If the interface stack has been unchanged since the last reinitialization of the local network management subsystem, then this object contains a zero value.
- **ifTableLastChange**—The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last reinitialization of the local network management subsystem, then this object contains a zero value.

Stacking Relationships for MPLS Layer Interfaces

The ifStackTable within the IF MIB provides a conceptual stacking relationship between the interfaces and subinterfaces represented as entries in the ifTable.

The ifStackTable is indexed like a linked list. Each entry shows a relationship between two interfaces providing the ifIndexes of the upper and the lower interface. The entries chain together to show the entire stacking relationship. Each entry links with one another until the stack terminates with an ifIndex of 0 at the highest and lowest ends of the stack. For example, in [Figure 1](#), the indexes .10.5 show that ifIndex 10 is stacked upon ifIndex 5. There are 0 entries at the highest and lowest ends of the stack; in [Figure 1](#), the indexes .0.15 and .72.0 are the highest and lowest ends of the stack, respectively.

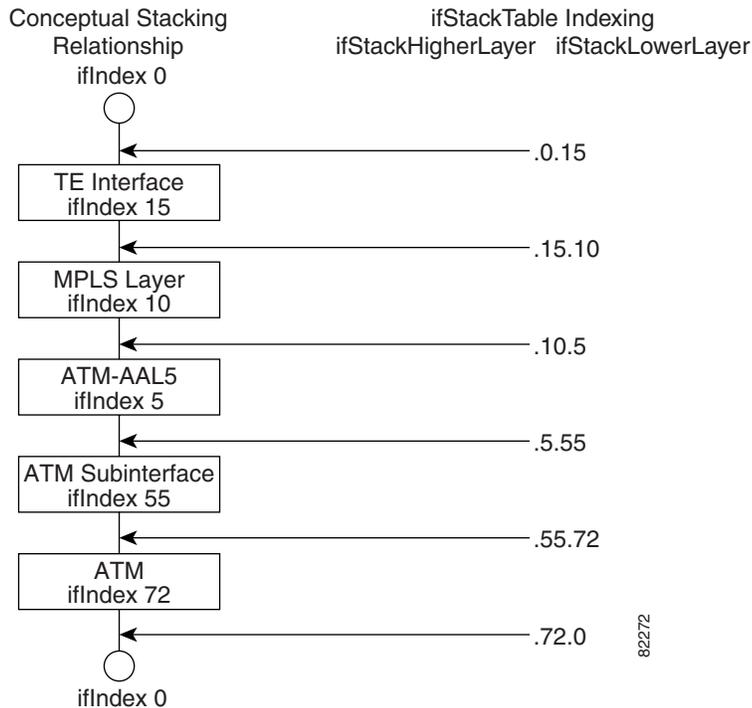
Figure 1 Sample ATM Stacking Relationship in the ifStackTable

Table 3 describes the indexing of the ifStackTable for the layer relationships shown in Figure 1.

**Note**

The order of the entries in Table 3 may not be the same as that seen in the MIB walk, which has to follow SNMP ordering rules.

Table 3 Layer Relationships

Layer Relationship (in Descending Order)	ifStackHigherLayer/ifStackLowerLayer
TE interface as top layer	.0.15
TE interface stacked upon MPLS layer	.15.10
MPLS layer stacked upon ATM-AAL5	.10.5
ATM-AAL5 layer stacked upon ATM subinterface	.5.55
ATM subinterface stacked upon ATM	.55.72
ATM as bottom layer	.72.0

Stacking Relationships for Traffic Engineering Tunnels

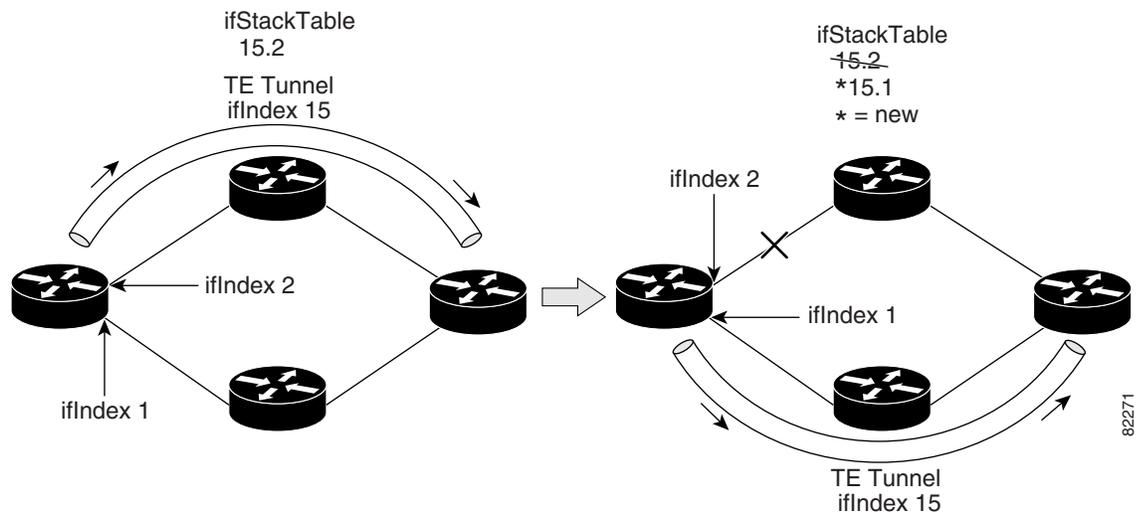
MPLS TE tunnels are represented in Cisco IOS software and the IF MIB as virtual interfaces. When properly signaled, TE tunnels pass traffic through MPLS over a physical interface. This process dictates that a TE tunnel is to be stacked on an MPLS layer that is stacked on an underlying interface.

TE tunnels can also change paths in response to different error or network conditions. These changes are instigated by using the RSVP-TE signaling protocol. When a change occurs, a tunnel can switch to a different MPLS interface. If no signaling path exists, no paths will be chosen and thus no MPLS interface will be used.

Because a TE tunnel is represented as an IF MIB ifTable entry, the ifStackTable also contains an entry corresponding to the TE tunnel. If the TE tunnel is successfully signaled, the ifStackTable also contains a link between the tunnel interface and one MPLS interface. Note that because it is possible for a TE tunnel to not have a corresponding signaled path, it is thus possible for a TE tunnel's ifStackTable entry to not have a corresponding lower layer. In this case, the lower layer variable contains the value of 0.

Figure 2 shows a TE tunnel before (left) and after (right) being rerouted and the effect on the ifStackTable. When ifIndex 2 fails, the TE tunnel is rerouted through ifIndex 1, the 15.2 entry is removed from the ifStackTable, and the 15.1 entry is added.

Figure 2 Sample TE Tunnel Stacking Relationship



MPLS Label Switching Router MIB Enhancements

All of the ifIndex references in the MPLS-LSR-MIB tables have changed from the ifIndex of the underlying physical or virtual interface to the ifIndex of the MPLS layer.

Table 4 shows the specific changes.

Table 4 MPLS-LSR-MIB ifIndex Objects Enhanced

Table	ifIndex
MPLS interface configuration table (mplsInterfaceConfTable)	mplsInterfaceConfIndex
MPLS in-segment table (mplsInSegmentTable)	mplsInSegmentIfIndex
MPLS cross-connect table (mplsXCTable)	mplsInSegmentIfIndex
MPLS out-segment table (mplsOutSegmentTable)	mplsOutSegmentIfIndex

The following objects from the mplsInterfaceConfTable are affected:

- `mplsInterfaceOutPackets`—Count only MPLS-encapsulated out packets
- `mplsInterfaceInPackets`—Count only MPLS-encapsulated in packets

Benefits of the MPLS Enhancements to Interfaces MIB

Improved Accounting Capability

By viewing the MPLS layer, you get MPLS-encapsulated traffic counters that do not include non-MPLS encapsulated traffic (for example, IP packets). Therefore, the counters are more useful for MPLS-related statistics.

TE Tunnel Interfaces

For TE tunnel interfaces, the stacking relationship reflects the current underlying MPLS interface that is in use and dynamically changes as TE tunnels reoptimize and reroute.

MPLS-Specific Information

The MPLS layer shows MPLS-specific information including the following:

- If MPLS is enabled
- MPLS counters
- MPLS MTU
- MPLS operational status

How to Configure MPLS Enhancements to Interfaces MIB

This section contains the following procedures:

- [Enabling the SNMP Agent, page 8](#) (required)
- [Configuration Examples for the MPLS Enhancements to Interfaces MIB, page 10](#) (optional)

Enabling the SNMP Agent

Perform the following task to enable the SNMP agent.

SUMMARY STEPS

1. `enable`
2. `show running-config`
3. `configure terminal`
4. `snmp-server community string [view view-name] [ro] [number]`
5. `end`
6. `write memory`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>show running-config</p> <p>Example: Router# show running-config</p>	<p>Displays the running configuration of the router so that you can determine if an SNMP agent is already running on the device.</p> <p>If no SNMP information is displayed, continue with the next step.</p> <p>If any SNMP information is displayed, you can modify the information or change it as desired.</p>
Step 3	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 4	<p>snmp-server community <i>string</i> [view <i>view-name</i>] [ro] [<i>number</i>]</p> <p>Example: Router(config)# snmp-server community public ro</p>	<p>Configures read-only (ro) community strings for the MPLS Label Distribution Protocol (LDP) MIB.</p> <ul style="list-style-type: none"> The <i>string</i> argument functions like a password, permitting access to SNMP functionality on label switch routers (LSRs) in an MPLS network. The optional ro keyword configures read-only (ro) access to the objects in the MPLS LDP MIB.
Step 5	<p>end</p> <p>Example: Router(config)# end</p>	<p>Exits to privileged EXEC mode.</p>
Step 6	<p>write memory</p> <p>Example: Router# write memory</p>	<p>Writes the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.</p>
Step 7	<p>show running-config</p> <p>Example: Router# show running-config</p>	<p>Displays the running configuration of the router so that you can determine if an SNMP agent is already running on the device.</p> <p>If you see any snmp-server statements, SNMP has been enabled on the router.</p> <p>If any SNMP information is displayed, you can modify the information or change it as desired.</p>

Configuration Examples for the MPLS Enhancements to Interfaces MIB

This section provides the following configuration examples:

- [MPLS Enhancements to Interfaces MIB: Examples, page 10](#)

MPLS Enhancements to Interfaces MIB: Examples

The following example shows how to enable an SNMP agent:

```
Router# configure terminal  
Router(config)# snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*.

```
Router(config)# snmp-server community public
```

In the following example, read-only access is allowed for all objects to members of access list 4 that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro 4
```

Additional References

The following sections provide references related to the MPLS Enhancements to Interfaces MIB feature.

Related Documents

Related Topic	Document Title
SNMP commands	<ul style="list-style-type: none"> • Cisco IOS Network Management Command Reference, Release 12.4T • Cisco IOS Network Management Command Reference, Release 12.2SB • Cisco IOS Network Management Command Reference, Release 12.2SR
SNMP configuration	“Configuring SNMP support” in the Cisco IOS Network Management Configuration Guide , Release 12.4
A description of SNMP agent support in Cisco IOS software for the MPLS Label Switching Router MIB (MPLS-LSR-MIB)	MPLS Label Switching Router MIB
A description of SNMP agent support in Cisco IOS for the MPLS Traffic Engineering MIB (MPLS TE MIB)	MPLS Traffic Engineering (TE) MIB
Other documentation	<p>“Multiprotocol Label Switching (MPLS) Label Switch Router (LSR) Management Information Base,” Internet draft, January 2002 [draft-ietf-mpls-lsr-mib-08.txt]; Srinivasan, C., Viswanathan, A., and Nadeau, T.D.</p> <p>Note For information on using SNMP MIB features, see the appropriate documentation for your network management system.</p>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
Interfaces Group MIB (IF MIB)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1156	<i>Management Information Base for Network Management of TCP/IP-based internets</i>
RFC 1157	<i>A Simple Network Management Protocol (SNMP)</i>
RFC 1213	<i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II</i>
RFC 1229	<i>Extensions to the Generic-Interface MIB</i>
RFC 2233	<i>Interfaces MIB</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, use the *Cisco IOS Multiprotocol Label Switching Command Reference* at http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **snmp-server community**

Glossary

ATM—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

ATM-AAL5—ATM adaptation layer 5. One of four AALs recommended by the ITU-T. AAL5 supports connection-oriented variable bit rate (VBR) services and is used predominantly for the transfer of classical IP over ATM and LAN emulation (LANE) traffic. AAL5 uses simple and efficient AAL (SEAL) and is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability.

encapsulation—Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

IETF—Internet Engineering Task Force. A task force (consisting of more than 80 working groups) that is developing standards for the Internet and the IP suite of protocols.

interface—The boundary between adjacent layers of the ISO model.

label—A short, fixed-length identifier that is used to determine the forwarding of a packet.

label switching—A term used to describe the forwarding of IP (or other network layer) packets using a label swapping algorithm based on network layer routing algorithms. The forwarding of these packets uses the exact match algorithm and rewrites the label.

LSR—label switching router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

MIB—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MPLS—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

MPLS interface—An interface on which MPLS traffic is enabled.

MTU—maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

NMS—network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

OID—object identifier. Values are defined in specific MIB modules. The Event MIB allows you or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and Boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, you or an NMS configures a trigger entry in the `mteTriggerTable` of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and Boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both.

SNMP—Simple Network Management Protocol. A management protocol used almost exclusively in TCP/IP networks. SNMP provides a means for monitoring and controlling network devices, and for managing configurations, statistics collection, performance, and security.

traffic engineering tunnel—A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

trap—A message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps are less reliable than notification requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

tunnel—A secure communication path between two peers, such as routers.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, 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. (0805R)

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.

© 2004–2008 Cisco Systems, Inc. All rights reserved.



MPLS Label Switching Router MIB

The MPLS Label Switching Router MIB (MPLS-LSR-MIB) allows you to use the Simple Network Management Protocol (SNMP) to remotely monitor a label switch router (LSR) that is using the Multiprotocol Label Switching (MPLS) technology.

Scalability enhancements provided in the Cisco IOS 12.0(28)S release reduce the size of any MIB walk and improve the usability of the MPLS-LSR-MIB.

Feature History for MPLS Label Switching Router MIB

Release	Modification
12.0(14)ST	This feature was introduced on Cisco IOS Release 12.0(14)ST
12.2(2)T	This feature was integrated into Cisco IOS Release 12.2(2)T.
12.0(22)S	This feature was implemented on the Cisco 12000 series routers and integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S and implemented on Cisco 7200 and Cisco 7500 series routers.
12.2(25)S	This feature was updated to work in the MPLS High Availability environment with the Cisco 7500 series routers.
12.0(28)S	This feature was updated to include scalability enhancements in Cisco IOS Release 12.0(28)S.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

This document includes the following major sections:

- [Information About MPLS Label Switching Router MIB, page 2](#)
- [How to Configure the MPLS LSR MIB, page 14](#)
- [Configuration Examples for the MPLS LSR MIB, page 16](#)
- [Additional References, page 17](#)
- [Command Reference, page 18](#)
- [Glossary, page 18](#)

Information About MPLS Label Switching Router MIB

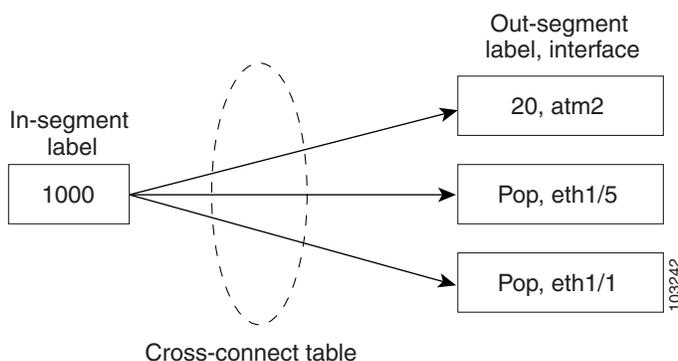
The MPLS-LSR-MIB contains managed objects that support the retrieval of label switching information from a router. The MIB is based on Revision 05 of the IETF MPLS-LSR-MIB. The MPLS-LSR-MIB mirrors a portion of the Cisco MPLS subsystem; specifically, it mirrors the Label Forwarding Information Base (LFIB). This implementation enables a network administrator to get information on the status, character, and performance of the following:

- MPLS-capable interfaces on the LSR
- Incoming MPLS segments (labels) at an LSR and their associated parameters
- Outgoing segments (labels) at an LSR and their associated parameters

In addition, the network administrator can retrieve the status of cross-connect table entries that associate MPLS segments with each other.

Figure 1 shows the association of the cross-connect table with incoming and outgoing segments (labels).

Figure 1 Label Forwarding with the Cross-Connect Table



Note

The out-segment table does not display “no label” entries. Labels that are displayed as “POP” are the special MPLS label 3.

The notation used in the MPLS-LSR-MIB follows the conventions defined in Abstract System Notation One (ASN.1). ASN.1 defines an Open System Interconnection (OSI) language used to describe data types apart from particular computer structures and presentation techniques. Each object in the MIB

incorporates a DESCRIPTION field that includes an explanation of the object's meaning and usage, which, together with the other characteristics of the object (SYNTAX, MAX-ACCESS, and INDEX) provides sufficient information for management application development, as well as for documentation and testing.

The MPLS-LSR-MIB represents an ASN.1 notation reflecting an idealized MPLS LSR.

A network administrator can access the entries (objects) in the MPLS-LSR-MIB by means of any SNMP-based network management system (NMS). The network administrator can retrieve information in the MPLS-LSR-MIB using standard SNMP **get** and **getnext** operations.

Typically, SNMP runs as a low-priority process. The response time for the MPLS-LSR-MIB is expected to be similar to that for other MIBs. The size and structure of the MIB and other MIBs in the system influence response time when you retrieve information from the management database. Traffic through the LSR also affects SNMP performance. The busier the switch is with forwarding activities, the greater the possibility of lower SNMP performance.

MPLS-LSR-MIB Elements

The top-level components of the MPLS-LSR-MIB consist of

- Tables and scalars (mplsLsrObjects)
- Traps (mplsLsrNotifications and mplsLsrNotifyPrefix)
- Conformance (mplsLsrConformance)

This Cisco implementation does not support the notifications defined in the MIB, nor does it support the labelStackTable or the trafficParamTable.

MPLS-LSR-MIB Tables

The Cisco implementation of the MPLS-LSR-MIB supports four main tables:

- Interface configuration
- In-segment
- Out-segment
- Cross-connect

The MIB contains three supplementary tables to supply performance information. This implementation does not support the label stack and traffic parameter tables.

The following sections list the MPLS-LSR-MIB tables (main and supplementary), their functions, table objects that are supported, and table objects that are *not* supported.

MPLS interface configuration table (mplsInterfaceConfTable)

Provides information for each MPLS-capable interface on an LSR.

Supports:

- A unique interface index or zero
- Minimum and maximum values for an MPLS label received on the interface
- Minimum and maximum values for an MPLS label sent from the interface
- A value for an MPLS label sent from the interface
- Per platform (0) or per interface (1) setting

- The storage type

Does not support:

- The total usable bandwidth on the interface
- The difference between the total usable bandwidth and the bandwidth in use

MPLS interface performance table (mplsInterfacePerfTable)

Augments the MPLS interface configuration table.

Supports:

- The number of labels in the incoming direction in use
- The number of top-most labels in outgoing label stacks in use

Does not support:

- The number of top-most labels in outgoing label stacks in use
- The number of labeled packets discarded because no cross-connect entries exist
- The number of outgoing MPLS packets requiring fragmentation for transmission

MPLS in-segment table (mplsInSegmentTable)

Contains a description of incoming segments (labels) at an LSR and their associated parameters.

Administrative and operational status objects for this table control packet transmission. If administrative and operational status objects are down, the LSR does not forward packets. If these status objects are up, the LSR forwards packets.

Supports:

- A unique index identifier
- The incoming label
- The number of labels to pop from the incoming segment
- An address family number from the Internet Assigned Number Authority (IANA)
- A segment cross-connect entry association
- The segment owner
- The storage type
- The administrative status
- The operational status



Note

The administrative status and operational status are always up for inSegments in the Cisco implementation. Otherwise, these entries do not appear in the table.

Does not support:

- A pointer to a traffic parameter table entry (set to the default 0.0)

MPLS in-segment performance table (mplsInSegmentPerfTable)

Augments the MPLS in-segment table, providing performance information and counters for incoming segments on an LSR.

Supports:

- The number of 32-bit octets received
- The number of 64-bit octets received
- The time of the last system failure that corresponded to one or more incoming segment discontinuities

**Note**

The lastFailure parameter is set to zero because it has no meaning in the Cisco implementation.

Does not support:

- The total number of packets received
- The number of packets with errors
- The number of labeled packets discarded with no errors

MPLS out-segment table (mplsOutSegmentTable)

Contains a description of outgoing segments from an LSR and their associated parameters.

Administrative and operational status objects for this table control packet transmission. If administrative and operational status objects are down, the LSR does not forward packets. If these values are up, the LSR forwards packets.

Supports:

- A unique index identifier
- An interface index of the outgoing interface
- An indication of whether or not a top label is pushed onto the outgoing packet's label stack
- The label to push onto the outgoing packet's label stack (if the previous value is true)
- The next hop address type
- The IPv4 address of the next hop
- The segment cross-connect entry association
- The segment owner
- The storage type
- The administrative status
- The operational status

**Note**

The administrative and operational status entries are always up in the Cisco implementation. Otherwise, the administrative and operational status entries do not appear in the table.

Does not support:

- An IPv6 address of the next hop
- A pointer to a traffic parameter table entry (set to the default 0.0)

MPLS out-segment performance table (mplsOutSegmentPerfTable)

Augments the MPLS out-segment table, providing performance information and counters for outgoing segments on an LSR.

Supports:

- The number of 32-bit octets sent
- The number of 64-bit octets sent
- The time of the last system failure that corresponded to one or more outgoing segment discontinuities

Does not support:

- The number of packets sent
- The number of packets that could not be sent because of errors
- The number of packets discarded with no errors

MPLS cross-connect table (mplsXCTable)

Associates inSegments (labels) with outSegments (labels) to show the manager how the LSR is currently swapping these labels.

A row in this table consists of one cross-connect entry that is indexed by the cross-connect index, the interface index of the incoming segment, the incoming label, and the out-segment index.

The administrative and operational objects for this table control packet forwarding to and from a cross-connect entry (XCEntry). The administrative status and operational status are always up in the Cisco implementation. Otherwise, the LSR would not forward packets.

Supports:

- A unique index identifier for a group of cross-connect segments
- A label switched path (LSP) to which the cross-connect entry belongs
- An index to the MPLS label stack table that identifies the stack of labels to be pushed under the top label
- An indication whether or not to restore the cross-connect entry after a failure (the default value is false)
- The cross-connect owner
- The storage type
- The administrative status (if up)
- The operational status (if up)

**Note**

The administrative status and operational status are always up in the Cisco implementation. Otherwise, these status entries do not appear in the table.

Does not support:

- Tunnel IDs as label switched path (LSP) ID objects

Information from Scalar Objects

The MPLS-LSR-MIB supports several scalar objects. In the Cisco implementation of the MIB, the following scalar objects are hard-coded to the value indicated and are read-only objects:

- `mplsOutSegmentIndexNext (0)`—The value for the out-segment index when an LSR creates a new entry in the MPLS out-segment table. The 0 indicates that this is not implemented because modifications to this table are not allowed.
- `mplsXCTIndexNext (0)`—The value for the cross-connect index when an LSR creates an entry in the MPLS cross-connect table. The 0 indicates that no unassigned values are available.
- `mplsMaxLabelDepth(2)`—The value for the maximum stack depth.
- `mplsLabelStackIndexNext (0)`—The value for the label stack index when an LSR creates entries in the MPLS label stack table. The 0 indicates that no unassigned values are available.
- `mplsTrafficParamIndexNext (0)`—The value for the traffic parameter index when an LSR creates entries in the MPLS traffic parameter table. The 0 indicates that no unassigned values are available.

The following scalar objects do not contain information for the MPLS-LSR-MIB and are coded as false:

- `mplsInSegmentTrapEnable (false)`—In-segment traps are not sent when this value is false.
- `mplsOutSegmentTrapEnable (false)`—Out-segment traps are not sent when this value is false.
- `mplsXCTrapEnable (false)`—Cross-connect traps are not sent when this value is false.

No trap information exists to support the MIB. Therefore, the following traps are not supported:

- `mplsInSegmentUp`
- `mplsInSegmentDown`
- `mplsOutSegmentUp`
- `mplsOutSegmentDown`
- `mplsXCUp`
- `mplsXCDown`

Linking Table Elements

In the cross-connect table, cross-connect entries associate incoming segments and interfaces with outgoing segments and interfaces. The following objects index the cross-connect entry:

- Cross-connect index—A unique identifier for a group of cross-connect entries in the cross-connect table. In the Cisco implementation, this value is always the same as that for the outSegmentIndex, unless there is no label or if the label has been popped.
- Interface index of the in-segment—A unique index for an entry in the in-segment table that represents an incoming MPLS interface. The value 0 means platform wide, for any entries that apply to all interfaces.
- Incoming label—An entry in the in-segment table that represents the label on the incoming packet.
- Out-segment index—A unique identifier for an entry in the out-segment table that contains a top label for the outgoing packet's label stack and an interface index of the outgoing interface.

Figure 2 shows the links between the in-segment and the out-segment in the cross-connect table.

Figure 2 Cross-Connect Table Links

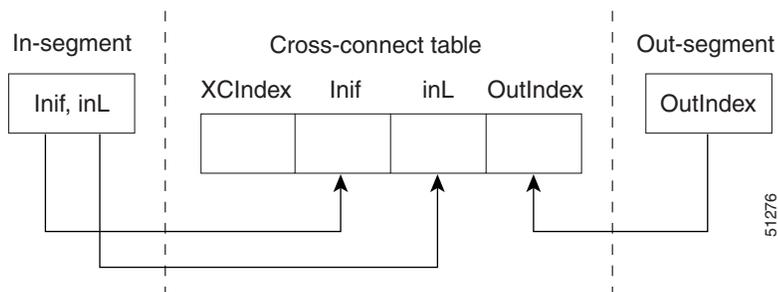


Table 1 shows the cross-connect table links you might see in the output from SNMP **get** operations on the MPLS-LSR-MIB objects that index a cross-connect entry. These objects include

- In-Segment Values—mplsInSegmentIfIndex and mplsInSegmentLabel
- Cross-Connect Entry—mplsXCIndex
- Out-Segment Values—mplsOutSegmentIndex

Table 1 *MPLS LSR Output Showing Cross-Connect Table Links*

In-Segment Values	Cross-Connect Entry	Out-Segment Values
0 ¹ , 1000	500 ² , 0, 1000, 0 ²	—
	501, 0, 1000, 501	501 = Pop (topLabel), Eth 1/5
	502, 0, 1000, 502	502 = Pop (topLabel), Eth, 1/1

1. All MPLS-enabled interfaces can receive incoming labels.
2. For this implementation of the MPLS-LSR-MIB, the cross-connect index and the out-segment index are the same. If there is no outsegment, the value will be zero.



Note

The OutSegmentIndex object is not the label. The label can be retrieved from the mplsOutSegmentTopLabel object.

Interface Configuration Table and Interface MIB Links

The MPLS interface configuration table lists interfaces that support MPLS technology. An LSR creates an entry dynamically in this table for each MPLS-capable interface. An interface becomes MPLS-capable when MPLS is enabled on that interface. A non-zero index for an entry in this table points to the ifIndex for the corresponding interface entry in the ifTable of the Interfaces Group MIB.

The ifTable contains information on each interface in the network. Its definition of an interface includes any sublayers of the internetwork layer of the interface. MPLS interfaces fit into this definition of an interface. Therefore, each MPLS-enabled interface is represented by an entry in the ifTable.

The interrelation of entries in the ifTable is defined by the interfaces stack group of the Interfaces Group MIB. Figure 3 shows how the stack table might appear for MPLS interfaces. The underlying layer refers to any interface that is defined for MPLS internetworking, for example, ATM, Frame Relay, or Ethernet.

Figure 3 *Interface Group MIB Stack Table for MPLS Interfaces*

MPLS-interface ifType = mpls(166)	51273
Underlying Layer . . .	

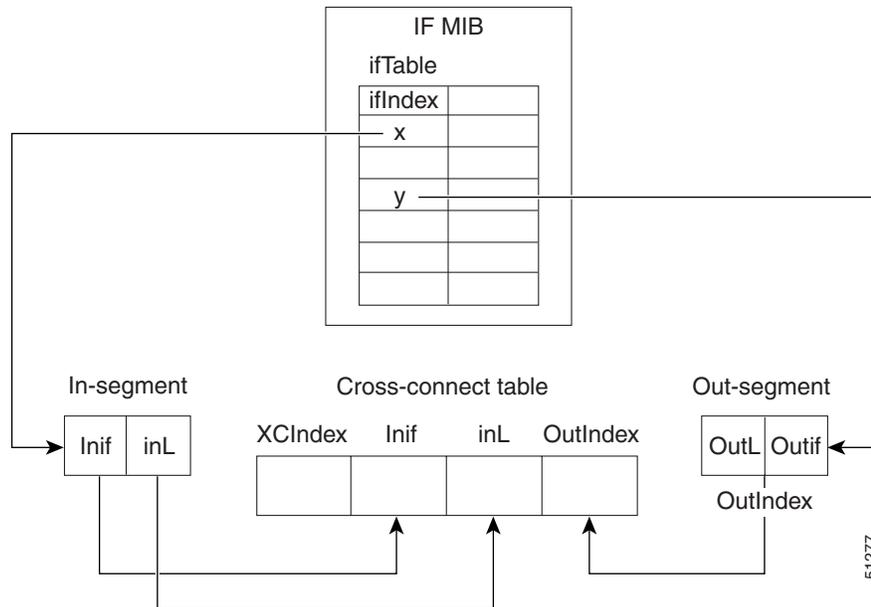


Note

Tunnel interfaces are included in the MPLS list for the current implementation.

The incoming and outgoing packets include a reference to the interface index for the ifTable of the Interfaces Group MIB. Figure 4 shows the links between MPLS-LSR-MIB objects and the Interfaces Group MIB.

Figure 4 MPLS-LSR-MIB and Interfaces Group MIB Links



- For the Interfaces Group MIB (IF MIB):
 - ifTable represents the MPLS interface table.
 - ifIndex represents the index to an entry in the MPLS interface table.
- For the In-segment:
 - Inif represents the interface on the incoming segment (references an index entry in the ifTable).
 - inL represents the label on the incoming segment.
- For the Out-segment:
 - OutL represents the label on the outgoing segment.
 - Outif represents the interface on the outgoing segment (references an index entry in the ifTable).
- For the Cross-connect table:
 - XCIndex represents the index to an entry in the MPLS cross-connect table.
 - Inif represents the interface on the incoming segment.
 - inL represents the MPLS label on the incoming segment.
 - OutIndex represents an index to an entry in the MPLS out-segment table.

Using the MPLS-LSR-MIB

The MPLS-LSR-MIB enables you to display the contents of the MPLS Label Forwarding Information Base (LFIB). It gives you the same information that you can obtain using the CLI command **show mpls forwarding-table**.

However, the MPLS-LSR-MIB approach offers these advantages over the CLI command approach:

- A more efficient use of network bandwidth
- Greater interoperability among vendors
- Greater security (SNMP Version 3)

The following paragraphs describe the MPLS-LSR-MIB structure and show, through the use of an example, how the two approaches to the information display compare.

MPLS-LSR-MIB Structure

MIB structure is represented by a tree hierarchy. Branches along the tree have short text strings and integers to identify them. Text strings describe object names, and integers allow computer software to encode compact representations of the names.

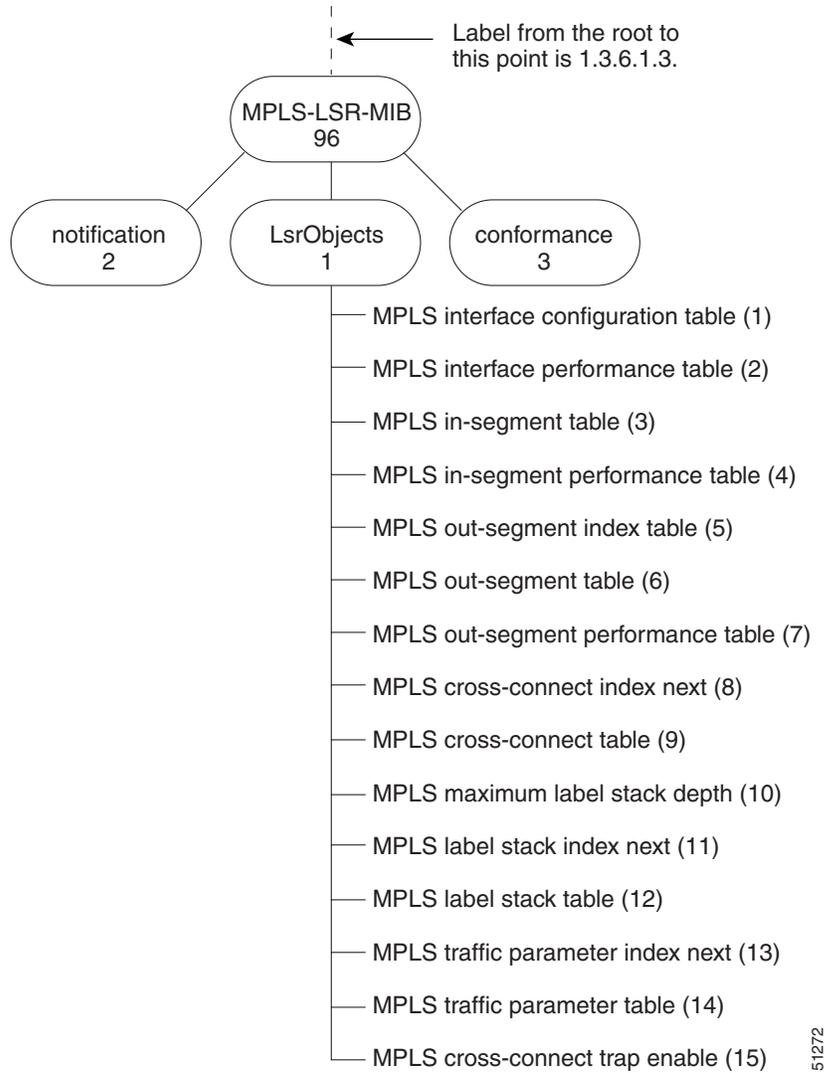
The MPLS-LSR-MIB falls on the experimental branch of the Internet MIB hierarchy. The experimental branch of the Internet MIB hierarchy is represented by the object identifier 1.3.6.1.3. This branch can also be represented by its object name *iso.org.dod.internet.experimental*. The MPLS-LSR-MIB is identified by the object name *mplsLsrMIB*, which is denoted by the number 96. Therefore, objects in the MPLS-LSR-MIB can be identified in either of the following ways:

- The object identifier—1.3.6.1.3.96.[MIB-variable]
- The object name—*iso.org.dod.internet.experimental.mplsLsrMIB.[MIB-variable]*

To display a *MIB-variable*, you enter an SNMP **get** command with an object identifier. Object identifiers are defined by the MPLS-LSR-MIB.

Figure 5 shows the position of the MPLS-LSR-MIB in the Internet MIB hierarchy.

Figure 5 MPLS-LSR-MIB in the Internet MIB Hierarchy



51272

CLI Commands and the MPLS-LSR-MIB

The MPLS LFIB is the component of the Cisco MPLS subsystem that contains management information for LSRs. You can access this management information by means of either of the following:

- Using the **show mpls forwarding-table** CLI command
- Entering SNMP **get** commands on a network manager

The following examples show how you can gather LSR management information using both methods.

CLI Command Output

A **show mpls forwarding-table** CLI command allows you to look at label forwarding information for a packet on a specific MPLS LSR.

```
Router# show mpls forwarding-table
```

Local Tag	Outgoing Tag or VC	Prefix or Tunnel Id	Bytes Tag Switched	Outgoing interface	Next Hop
19	Pop Tag	10.3.4.0/24	0	Et1/4	10.22.23.23
22	23	14.14.14.14/32	0	AT2/0.1	point2point
	1/36	14.14.14.14/32	0	AT2/0.2	point2point

MPLS-LSR-MIB Output

SNMP commands on MIB objects also allow you to look at the label forwarding information for a specific MPLS LSR.

You can do a walk-through of the MIB by running a command such as **getmany -v2c public mplsLsrMIB** on a network manager where **getmany** does repeated SNMP **getnext** operations to retrieve the contents of the MPLS-LSR-MIB.

```
mplsXCOperStatus.9729.0.19.9729 = up(1)
mplsXCOperStatus.11265.0.22.11265 = up(1)
mplsXCOperStatus.11266.0.22.11266 = up(1)
```

You can continue to scan the output of the **getmany** command for the following (from the MPLS out-segment table):

- Out-segment's top label objects (mplsOutSegmentTopLabel)

```
mplsOutSegmentTopLabel.9729 = 3
mplsOutSegmentTopLabel.11265 = 23
mplsOutSegmentTopLabel.11266 = 65572
```



Note

65572 is 1/36 in label form (1 is the high-order 16 bits. 36 is the low-order 16 bits.)

- Out-segment's interface index (mplsOutSegmentIfIndex)

```
mplsOutSegmentIfIndex.9729 = 7
mplsOutSegmentIfIndex.11265 = 28
mplsOutSegmentIfIndex.11266 = 31
```

Benefits

The benefits described in the following paragraphs are available to you with the MPLS-LSR-MIB.

Troubleshooting LSR Problems

By monitoring the cross-connect entries and the associated incoming and outgoing segments, you can see which labels are installed and how they are being swapped. Use the MPLS-LSR-MIB in place of the **show mpls forwarding** CLI command.

Monitoring of LSR Traffic Loads

By monitoring interface and packet operations on an MPLS LSR, you can identify high- and low-traffic patterns, as well as traffic distributions.

Improvement of Network Performance

By identifying potentially high-traffic areas, you can set up load sharing to improve network performance.

Verification of LSR Configuration

By comparing results from SNMP **get** commands and the **show mpls forwarding** CLI command, you can verify your LSR configuration.

Displaying of Active Label Switched Paths

By monitoring the cross-connect entries and the associated incoming segments and outgoing segments, you can determine the active LSPs.

How to Configure the MPLS LSR MIB

See the following sections for configuration tasks for the MPLS-LSR-MIB feature. Each task in the list is identified as either optional or required.

- [Enabling the SNMP Agent](#) (required)
- [Verifying That the SNMP Agent Has Been Enabled](#) (optional)

Prerequisites

The MPLS-LSR-MIB requires the following:

- SNMP installed and enabled on the LSR
- MPLS enabled on the LSR
- 60K of memory



Note Additional capacity is not required for runtime dynamic random-access memory (DRAM).

Enabling the SNMP Agent

The SNMP agent for the MPLS-LSR-MIB is disabled by default. To enable the SNMP agent, perform the following steps:

SUMMARY STEPS

1. **enable**
2. `show running-config`
3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro**] [*number*]
5. **end**
6. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>show running-config</code> Example: Router# show running-config	Displays the running configuration of the router to determine if an SNMP agent is already running on the device. If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as desired.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	snmp-server community <i>string</i> [view <i>view-name</i>] [ro] [<i>number</i>] Example: Router(config)# snmp-server community public ro	Configures read-only (ro) SNMP community strings. This command enables the SNMP agent and permits any SNMP manager to access all objects with read-only permission using the community string public.

	Command or Action	Purpose
Step 5	<code>end</code> Example: Router(config)# <code>end</code>	Exits to privileged EXEC mode.
Step 6	<code>copy running-config startup-config</code> Example: Router# <code>copy running-config startup-config</code>	Copies the modified SNMP configuration into router NVRAM, permanently saving the SNMP settings. When you are working with Cisco IOS Release 10.3 or earlier, use the write memory command.

Verifying That the SNMP Agent Has Been Enabled

To verify that the SNMP agent has been enabled, perform the following steps:

-
- Step 1** Access the router through a Telnet session:
- ```
Prompt# telnet xxx.xxx.xxx.xxx
```
- where `xxx.xxx.xxx.xxx` represents the IP address of the target device.
- Step 2** Enter privileged mode:
- ```
Router# enable
```
- Step 3** Display the running configuration and look for SNMP information:
- ```
Router# show running-configuration
...
...
snmp-server community public RO
```

If you see any “snmp-server” statements, SNMP has been enabled on the router.

---

## Configuration Examples for the MPLS LSR MIB

The following example shows how to enable an SNMP agent.

```
configure terminal
snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*.

```
configure terminal
snmp-server community public
```

In the following example, read-only access is allowed for all objects to members of access list 4 that specify the *comaccess* community string. No other SNMP managers have access to any objects.

```
configure terminal
snmp-server community comaccess ro 4
```

# Additional References

The following sections provide references related to the MPLS LSR MIB.

## Related Documents

| Related Topic                             | Document Title                                                                                                                                                                                                                                                      |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring SNMP using Cisco IOS software | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Network Management Configuration Guide, Release 12.4</a>, Configuring SNMP Support</li> <li>• <a href="#">Cisco IOS Network Management Command Reference, Release 12.4</a>, SNMP Commands</li> </ul> |

## Standards

| Standard                       | Title                                                            |
|--------------------------------|------------------------------------------------------------------|
| draft-ietf-mpls-lsr-mib-05.txt | MPLS Label Switch Router Management Information Base Using SMIV2 |
| draft-ietf-mpls-arch-07.txt    | Multiprocol Label Switching Architecture                         |

## MIBs

| MIBs                                                                                               | MIBs Link                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• MPLS Label Switching Router MIB (MPLS-LSR-MIB)</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs                                                                                                                    | Title                                 |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| The LSR implementation supporting the MPLS-LSR-MIB is in full compliance with all provisions of Section 10 of RFC 2026. | <i>The Internet Standards Process</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

This feature uses no new or modified commands.

## Glossary

**cross-connect (XC)**—An association of in-segments and incoming Multiprotocol Label Switching (MPLS) interfaces to out-segments and outgoing MPLS interfaces.

**IETF**—Internet Engineering Task Force. A task force (consisting of more than 80 working groups) that is developing standards for the Internet and the IP suite of protocols.

**inSegment**—A label on an incoming packet that is used to determine the forwarding of the packet.

**Internet Engineering Task Force**—See IETF.

**label**—A short, fixed length identifier that is used to determine the forwarding of a packet.

**Label Distribution Protocol**—See LDP.

**label switched path**—See LSP.

**label switching**—Describes the forwarding of IP (or other network layer) packets by a label swapping algorithm based on network layer routing algorithms. The forwarding of these packets uses the exact match algorithm and rewrites the label.

**label switch router**—See LSR.

**LDP**—Label Distribution Protocol. A standard protocol that operates between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LSP**—label switched path. A sequence of hops in which a packet travels from one router to another router by means of label switching mechanisms. A label switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

**LSR**—label switch router. A device that forwards Multiprotocol Label Switching (MPLS) packets based on the value of a fixed-length label encapsulated in each packet.

**Management Information Base**—See MIB.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP). The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic through use of a label. This label instructs the routers and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information.

**MPLS interface**—An interface on which Multiprotocol Label Switching (MPLS) traffic is enabled.

**Multiprotocol Label Switching**—See MPLS.

**notification request**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal, indicating that a significant event occurred. SNMP notification requests are more reliable than traps, because a notification request from an SNMP agent requires that the SNMP manager acknowledge receipt of the notification request. The manager replies with an SNMP response protocol data unit (PDU). If the manager does not receive a notification message from an SNMP agent, it does not send a response. If the sender (SNMP agent) never receives a response, the notification request can be sent again.

**outSegment**—A label on an outgoing packet.

**Simple Network Management Protocol**—See SNMP.

**SNMP**—Simple Network Management Protocol. A management protocol used almost exclusively in TCP/IP networks. SNMP provides a means for monitoring and controlling network devices, and for managing configurations, statistics collection, performance, and security.

**trap**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps are less reliable than notification requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

**Note**

---

Refer to the Cisco [Dictionary of Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS QoS Multi-VC Mode for PA-A3

---

## Feature History

| Release   | Modification                                                                            |
|-----------|-----------------------------------------------------------------------------------------|
| 12.2(1)T  | This feature was introduced on the Cisco IOS Release 12.2(1)T.                          |
| 12.2(4)T  | Added support for the Cisco MGX 8850 and MGX 8950 switch with a Cisco MGX RPM-PR card.  |
| 12.2(4)T2 | Support for the Cisco 7500 series routers added.                                        |
| 12.4(20)T | Support was removed for this feature in Cisco IOS Release 12.4(20)T and later releases. |

This document describes the MPLS QoS Multi-VC Mode for PA-A3 feature being made available to customers for use with Cisco IOS Release 12.2(4)T. This document contains the following sections:

- [Feature Overview](#)
- [Supported Platforms](#)
- [Supported Standards, MIBs, and RFCs](#)
- [Prerequisites](#)
- [Configuration Tasks](#)
- [Configuration Examples](#)
- [Command Reference](#)
- [Glossary](#)

## Feature Overview

MPLS quality of service (QoS) functionality enables network administrators to satisfy a wide range of requirements in transmitting IP packets through an MPLS-enabled network. Table 1 contains a brief summary of three primary MPLS QoS service offerings made available to customers through earlier Cisco IOS releases.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

**Table 1**      **MPLS QoS Services**

| <b>Service Category</b> | <b>Service Function</b>                                                                                                                                      | <b>Service Description</b>                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packet classification   | Committed access rate (CAR). Packets are classified at the edge of the network before labels are assigned.                                                   | CAR uses the type of service (ToS) bits in the IP header to classify packets according to input and output transmission rates. CAR is often configured on interfaces at the edge of a network to control the flow of traffic into or out of the network. You can use CAR commands to classify or reclassify a packet. |
| Congestion avoidance    | Weighted random early detection (WRED). Packet classes are differentiated based on drop probability.                                                         | WRED monitors network traffic to anticipate and prevent congestion at common network and internetwork bottlenecks. WRED can selectively discard lower priority traffic when an interface is congested; WRED can also provide differentiated performance characteristics for different classes of service.             |
| Congestion management   | Class-based weighted fair queueing (CBWFQ). Packet classes are differentiated based on bandwidth requirements and finite transmission delay characteristics. | CBWFQ is an automated scheduling system that ensures fair bandwidth allocation to all network traffic. CBWFQ uses weights (priorities) to determine how much bandwidth is allocated to each class of traffic.                                                                                                         |

For more information about configuring the MPLS QoS services summarized in [Table 1](#), see the *Cisco IOS Quality of Service Solutions Configuration Guide*.

For complete command syntax information for configuring CAR, WRED, and CBWFQ functionality, see the *Cisco IOS Quality of Service Solutions Command Reference*.

In general, MPLS QoS enables the duplication of Cisco IOS IP QoS (Layer 3) functions on MPLS devices, including label edge routers (LERs), label switching routers (LSRs), and Asynchronous Transfer Mode LSRs (ATM-LSRs). MPLS QoS functions map nearly one-for-one to IP QoS functions on all types of interfaces.

The MPLS QoS Multi-VC Mode functionality described in this document significantly enhances the generalized MPLS QoS capabilities outlined in [Table 1](#). Specifically, this new MPLS QoS feature enables users to map the experimental (EXP) field value of an MPLS label to an ATM virtual circuit (VC) to create sets of labeled virtual circuits (LVCs). Each set consists of multiple LVCs, and each LVC is treated as a member of the set.

All members of a set are associated with a label-switched path (LSP) that is set up between a pair of ATM-connected routers in the user's networking environment, and each member of a set has a different quality of service (QoS) from other members of the set.

By means of multi-VC sets, differentiated services can be provided to users of MPLS-enabled service provider networks. This service differentiation is accomplished by setting an appropriate value in the experimental (EXP) field in the header of each incoming packet as it is received by the provider edge (PE) router in the service provider network. This process is discussed in greater detail in the [“Optionally Setting the MPLS Experimental Field Value”](#) section.

The multi-VC mode functionality described in this document is used in conjunction with the Cisco Enhanced ATM Port Adapter (PA-A3) on a Cisco 7200 series router or a Cisco 7500 series router.

## Benefits

The MPLS QoS Multi-VC Mode feature provides the following significant benefits:

- Ensures effective deployment of differentiated service classes in an MPLS-enabled ATM network.
- Leverages the use of existing ATM infrastructures.

## Tag Switching/MPLS Terminology

Table 2 lists existing tag switching terms and the corresponding MPLS IETF terms used in this document and other related Cisco publications.

**Table 2**      *Equivalent Tag Switching and MPLS Terms*

| Old Designation                        | New Designation                                                                                                                                                                                                                                                                |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tag bit rate (TBR)                     | Label bit rate (LBR)                                                                                                                                                                                                                                                           |
| Tag switching                          | Multiprotocol Label Switching                                                                                                                                                                                                                                                  |
| Tag (short for tag switching)          | MPLS                                                                                                                                                                                                                                                                           |
| Tag (item or packet)                   | Label                                                                                                                                                                                                                                                                          |
| TDP (Tag Distribution Protocol)        | LDP (Label Distribution Protocol). Cisco TDP and LDP (MPLS Label Distribution Protocol) closely parallel each other in function, but differ in detail, such as message formats and the commands required to configure the respective protocols and to monitor their operation. |
| Tag switched                           | Label switched                                                                                                                                                                                                                                                                 |
| TFIB (tag forwarding information base) | LFIB (label forwarding information base)                                                                                                                                                                                                                                       |
| TSR (tag switching router)             | LSR (label switching router)                                                                                                                                                                                                                                                   |
| TSC (tag switch controller)            | LSC (label switch controller)                                                                                                                                                                                                                                                  |
| ATM-TSR (ATM tag switch router)        | ATM-LSR (ATM label switch router), for example, BPX 8650                                                                                                                                                                                                                       |
| TVC (tag VC, tag virtual circuit)      | LVC (label VC, label virtual circuit)                                                                                                                                                                                                                                          |
| TSP (tag switch path)                  | LSP (label switch path)                                                                                                                                                                                                                                                        |
| XTagATM (extended tag ATM)             | XmplsATM (extended mpls ATM)                                                                                                                                                                                                                                                   |

## MPLS QoS Support in an MPLS Network

Several different possibilities exist for using MPLS QoS in an MPLS-enabled networking environment. The method you choose depends on whether the core of the network contains label switching routers (LSRs) or ATM label switch routers (ATM-LSRs). In either case, the QoS services provided are the same (the CAR, WRED, and CBWFQ services described in Table 1).

This section describes how LSRs and ATM-LSRs can be deployed to take advantage of QoS functions in an MPLS network:

- [LSRs Used at the Edge of an MPLS Network](#)
- [LSRs Used in the Core of an MPLS Network](#)

- [ATM-LSRs Used in the Core of an MPLS Network](#)
- [ATM Switches Used Without MPLS Enabled](#)

## LSRs Used at the Edge of an MPLS Network

LSRs used at the edge of an MPLS network backbone are usually Cisco 7200 or Cisco 7500 series routers running MPLS software. Edge LSRs can operate at either the ingress or the egress side of an MPLS network, as described below.

At the ingress side of an MPLS network, LSRs process packets as follows:

1. IP packets enter the edge of the MPLS network at the edge LSR.
2. The edge LSR uses CAR or some other IP packet classification mechanism, such as Modular QoS CLI (on the Cisco series 7200 and 7500 routers only), to classify incoming IP packets and to set the IP precedence value. Note that IP packets can be received with the IP precedence value already set.
3. For each incoming packet, the LSR performs a lookup on the IP address to determine the next-hop LSR.
4. The appropriate label is inserted into the packet, and the IP precedence bits are copied into the MPLS EXP field in the label header.
5. The labeled packets are forwarded to the appropriate output interface on the LSR for processing.
6. The packets are differentiated by class according to one of the following:
  - Drop probability—WRED
  - Bandwidth allocation and delay—CBWFQ

In either case, the edge LSR enforces the defined differentiation by continuing to employ WRED or CBWFQ on every ingress router.

At the egress side of an MPLS network, LSRs process packets as follows:

1. MPLS-labeled packets arrive at the egress LSR from the MPLS network backbone.
2. The MPLS labels are removed from the packets and the packets are classified.
3. For each IP packet, the egress LSR performs a lookup on the IP address to determine the packet's destination; the egress LSR then forwards the packet to the appropriate destination interface for processing.
4. The packets are differentiated according to the IP precedence values and treated accordingly, depending on the WRED or CBWFQ drop probability configuration.

## LSRs Used in the Core of an MPLS Network

LSRs used in the core of an MPLS network are usually Cisco 12000 series routers or Cisco 7500 series routers running MPLS software. Such routers process packets as follows:

1. Incoming MPLS labeled packets from an edge LSR (or other core device) arrive at the core LSR.
2. A table lookup is done by the core LSR to determine the next-hop LSR.
3. An appropriate label is placed (swapped) into the packet and the MPLS EXP bits are copied into the label header.
4. The labeled packet is then forwarded to the output interface of the core LSR for processing.
5. The outbound packet is differentiated by the MPLS EXP field marking and treated accordingly, depending on the WRED or CBWFQ configuration.

LSRs used in the core of an MPLS network implement the multiple LVC model. In this model, one label is assigned for each service class for each destination.

The operation of a core LSR is the same as that described in the preceding section for an edge LSR, except that the output of the core LSR is directed to an ATM interface.

WRED is used to define service classes and determine discard policy during periods of network congestion. CBWFQ is used to define the amount of bandwidth available for each class of service, enabling MPLS packets to be scheduled for transmission by traffic class during periods of network congestion.

## ATM-LSRs Used in the Core of an MPLS Network

ATM-LSRs in the core of a service provider MPLS network also implement the multiple LVC model. Such devices differentiate classes using weighted fair queuing (WFQ) techniques, which cause packets to be discarded intelligently during periods of network congestion to stabilize network behavior.

By means of a Cisco 7200 or Cisco 7500 router that incorporates the PA-A3 Enhanced ATM port adapter (see [Figure 2](#)), the service provider can configure the policy map to set the cell loss priority (CLP) bit in the header of ATM cells traversing the network, based on a matched value in the EXP field of the IP packet header. To effect the setting of the CLP bit in ATM cell headers, the service provider executes a **set atm-clp** command on an upstream router in the service provider's MPLS network.

The service provider can choose to set the CLP bit, as described above. Based on the setting of the most significant bit of the EXP field in the IP packet header, the ATM-LSR in the core of the service provider network can use the CLP bit to preferentially discard ATM cells during periods of congestion. Thus, setting the CLP bit in the header of ATM cells traversing the service provider's network ensures consistent packet/ATM cell discard treatment among the IP routers and ATM switches in the network.

On an IP router, the WRED congestion avoidance algorithm discards packets based on one of eight different values that can be assigned using the two least significant bits (LSBs) of the EXP field in the IP packet header. The values assigned to these two bits of the EXP field are used to define the packet's class, while the most significant bit (MSB) of the field is used to differentiate whether a packet entering the service provider network from a customer is "in rate" or "out of rate." Thus, the MSB of the EXP field enables the user to establish a desired WRED profile, causing packets to be discarded more aggressively during congestion conditions, provided that such packets are marked as being "out of rate."

As a necessary precondition, IP packets can be marked on the input interface of an edge router to ensure desired packet discard behavior in the event of congestion on the router's output interface. Similarly, for ATM cells traversing the core of the service provider's network, appropriate cell discard activity can be ensured by setting the CLP bit in ATM cell headers as the cells pass through a given ATM-LSR into the core of the service provider's network.

Thus, the CLP mechanism can be used to ensure that the ATM switches in the core of the service provider's network exhibit the same discard behavior as the routers on the edge of the network. The only difference is that the edge routers deal with IP packets, while the core switches deal with ATM cells.

## ATM Switches Used Without MPLS Enabled

When the core network uses ATM switches and the edge of the network uses MPLS-enabled edge LSRs, the edge LSRs are interconnected through a mesh of ATM Forum permanent virtual circuits (PVCs) involving constant bit rate (CBR) traffic, variable bit rate (VBR) traffic, or unspecified bit rate (UBR) traffic over the ATM core switches. The edge LSRs invoke WFQ on a per-VC basis to provide differentiation based on the delay characteristics of each type of QoS traffic multiplexed onto the ATM Forum PVC. Optionally, WRED can also be used on a per-VC basis to manage packet drop priority between classes when congestion occurs on the edge LSR.

## Using MPLS QoS in ATM Backbone

You realize the following benefits when you use MPLS QoS in a backbone consisting of ATM switches running MPLS:

- **Efficient resource allocation**—Class-based weighted fair queueing (CBWFQ) is used to allocate bandwidth on a per-class and per-link basis, thereby guaranteeing a percentage of link bandwidth for network traffic.
- **Connectionless environment**—If you implement MPLS QoS in your ATM backbone, you can avoid configuration of end-to-end PVCs for each class of service. This is especially advantageous when you integrate MPLS QoS services in your network in conjunction with MPLS VPN services.
- **Flexibility without additional overhead**—MPLS QoS promotes efficient use of bandwidth, enabling unused bandwidth to be allocated for other purposes. Also, MPLS QoS requires no call setup procedures because reachability is determined and appropriate resource allocation is accomplished before MPLS QoS services are initiated.

## Related Features and Technologies

You can use MPLS QoS with:

- MPLS virtual private networks (VPNs)
- Any MPLS network

## Related Documents

For additional information about MPLS functionality running on Cisco routers or switches in an MPLS environment, consult the following documentation:

- *MPLS Label Distribution Protocol*—This document describes the use of the MPLS Label Distribution Protocol (LDP), which enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding along normally routed paths. LDP supports the dynamic creation of different routes between source and destination nodes in a network, thus enabling IP services to be provided efficiently over Internet backbones.
- *Multiprotocol Label Switching on Cisco Routers*—This document describes a generic set of CLI commands used for configuring and monitoring MPLS functionality on Cisco routers and switches in an MPLS operating environment.
- *MPLS Label Switch Controller*—This document describes the use of a label switch controller (LSC) that operates in conjunction with a Cisco BPX 8650 IP+ATM switch to deliver scalable integration of IP services over an ATM network. An LSC supports rapid and direct implementation of advanced IP services over ATM networks that incorporate BPX 8650 switches. MPLS combines the performance and virtual circuit capabilities of Layer 2 (data link layer) switching with the scalability of Layer 3 (network layer) routing. This delivers a solution to service providers that supports rapid growth and provides differentiated services, while leveraging the use of existing network infrastructures.
- *MPLS Class of Service Enhancements*—This document describes how the IP precedence field (the first three bits of the DSCP field in the IP packet header) is used to specify the class of service when a customer transmits IP packets from one site to another through a service provider network. Based on this IP precedence marking, the packet is given specified treatment for that class of service as the packet traverses the service provider network. However, if the service provider network is an MPLS

network, the IP precedence bits in each packet are copied into the MPLS EXP field as the packet enters the edge of the service provider network. If the service provider wants to set an MPLS packet's class of service to a different value, based on a particular service offering, the service provider can set the MPLS EXP field rather than overwriting the value in the packet's IP precedence field. Thus, the IP packet header remains available for customer use, and the class of service for the IP packet is not changed as the packet traverses the MPLS network.

- *MPLS Virtual Private Networks (VPNs)*—This document describes how users can deploy and administer IPv4 Layer 3, value-added services and business applications across a public network infrastructure. Deploying business applications on a broad scale over WANs enables MPLS VPN users to reduce costs, increase revenue, and develop new business opportunities.
- *Quality of Service Solutions Configuration Guide*—This document describes the quality of service (QoS) features in Cisco IOS and the service models by which QoS functionality is delivered. It also outlines the benefits that come from incorporating QoS functionality in your network and describes the Cisco IOS features that ensure better services to selected network traffic in Frame Relay, ATM, Ethernet, SONET, and IP-routed networks.
- *Modular Quality of Service Command Line Interface*—This document describes how to configure QoS functionality using the Modular QoS CLI. Three basic QoS configuration tasks are described in this document: a) how to define a traffic class containing match criteria; b) how to create a service policy; and c) how to attach the service policy to an interface and specify the direction in which the service policy is to be applied to network traffic (either to packets entering an interface or to packets exiting an interface). The Modular QoS CLI enables users to specify traffic classes independently of QoS policies.

## Supported Platforms

The MPLS Class of Service Multi-VC Mode feature is supported in Cisco IOS Release 12.2(4)T on the following platforms that are equipped with the Enhanced Asynchronous Transfer Mode (ATM) Port Adapter (ATM PA-A3):

- Cisco 7200 series routers
- Cisco 7500 series routers (supported for Cisco IOS Release 12.2(4)T3 and later)

The ATM PA-A3 is a single-port, single- and dual-wide ATM port adapter used with the Cisco 7200 and 7500 series routers. It is designed with a high-performance, dual segmentation and reassembly (SAR) architecture with local buffer memory.

A Cisco 7200 series router or a Cisco 7500 series router equipped with an ATM PA-A3 port adapter can interoperate in multi-VC mode with the following Cisco ATM switches located in the core of an MPLS network:

- Cisco LS1010 ATM switch
- Cisco Catalyst 8540 MSR
- Cisco BPX 8650 series of ATM switches
- Cisco MGX 8800 series of ATM switches

The MPLS QoS Multi-VC Mode feature is also supported on the Cisco MGX 8850 switch with the Cisco MGX 8850 Route Processor Module (RPM-PR).

### Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

### Standards

No new or modified standards are supported by this feature.

### MIBs

No new or modified MIBs are supported by this feature.

### RFCs

No new or modified RFCs are supported by this feature.

## Prerequisites

To use MPLS QoS to full advantage in your network, the following functionality must be supported:

- Multiprotocol Label Switching (MPLS)—MPLS is the standardized label switching protocol defined by the Internet Engineering Task Force (IETF).
- Cisco Express Forwarding (CEF)—CEF is an advanced Layer 3 IP switching technology that optimizes performance and scalability in networks that handle large volumes of traffic and exhibit dynamic traffic patterns.
- Asynchronous Transfer Mode (ATM)—ATM signaling support is required if you use ATM interfaces in your network.




---

**Note** If you use only packet interfaces in your network, ATM functionality is not required.

---

- Quality of service (QoS) features supported in this release:
  - MPLS QoS Multi-VC mode feature—This feature provides QoS functionality on ATM interfaces in a service provider MPLS-enabled network. Such a network incorporates ATM interfaces on the edge of the network, as well as ATM interfaces within the core of the network.

IP packets travel through the core of an MPLS-enabled service provider network by means of multiple, label switched paths (LSPs), also known as label virtual circuits (LVCs), that are automatically established for each IP destination prefix. A standard IP access control list (ACL) is used to specify the number of traffic classes per IP destination, and hence the number of LVCs that will be created.

If there are multiple, equal cost paths through an ATM network, it is possible that each LVC relating to the same destination could take a different path through the network, because each LVC could be set up along an alternate, equal cost path. For example, if four equal cost paths exist through the network, the first LVC would be set up along the first path, the second LVC would be set up along the second path, and so forth. There is no guarantee, however, that each LVC would be set up along a *parallel* path in the network, nor is there any requirement that each LVC be set up in such a manner.

Each MPLS-enabled ATM interface in the service provider network, including each ATM edge interface and each ATM router/switch interface within the core of the network, provides QoS support in a manner similar to that provided for IP packet interfaces.

IP packets transiting the service provider's MPLS-enabled network are treated with the same priorities as afforded to ATM traffic. Accordingly, MPLS QoS multi-VC mode functionality is virtually indistinguishable from the QoS support provided for IP packet interfaces.

- Class-based weighted fair queueing (CBWFQ)—CBWFQ is a dynamic scheduling method that allocates bandwidth fairly to all network traffic. CBWFQ applies priorities, or weights, to traffic to classify the traffic into *flows* and determine how much bandwidth to allow each flow. WFQ moves interactive traffic to the front of a queue to reduce response time and fairly shares the remaining bandwidth among high-bandwidth flows.
- Weighted random early detection (WRED)—WRED is a congestion avoidance mechanism that extends random early detection (RED) functionality by allowing different discard priorities or classes of service to be configured per the MPLS experimental (EXP) field in the MPLS packet header. The EXP field value defines the relative importance or priority of an MPLS packet. The WRED mechanism uses the EXP field values to classify packets into any one of eight different discard priorities or classes of service to avoid congestion in an MPLS network.

## Configuration Tasks

The following sections describe configuration tasks for using the MPLS QoS multi-VC mode feature:

- (Required) [Configuring Cisco Express Forwarding](#)
- (Optional) [Optionally Setting the MPLS Experimental Field Value](#)
  - [Classifying Packets](#)
  - [Packet Prioritization](#)
  - [Using Modular QoS CLI to Configure Ingress Label Switching Router](#)
  - [Using CAR to Configure Ingress Label Switching Router](#)
- (Optional) [Configuring Class of Service for IP Packets on Output](#)
- (Required) [Configuring MPLS QoS in Core of ATM Network](#)
  - (Required) [Configuring Multi-VC Mode in MPLS-Enabled Network](#)
  - (Optional) [Configuring Multi-VCs Using the QoS-Map Function](#)
- (Optional) [Configuring Queueing Functions on Router Output Interfaces](#)

- [Configuring CBWFQ on Cisco 7200/7500 Series and Cisco MGX RPM-PR Router Interfaces](#)
- [Configuring WRED on Cisco 7200/7500 Series or Cisco MGX RPM-PR Router Interfaces](#)
- (Optional) [Verifying QoS Configuration on ATM Interfaces](#)

## Configuring Cisco Express Forwarding

Cisco Express Forwarding (CEF) is a prerequisite for using MPLS in the core of a network; CEF must be running on all the routers in the MPLS network. To enable CEF on the routers in an MPLS network, issue the appropriate command on each device, as indicated in [Table 3](#).

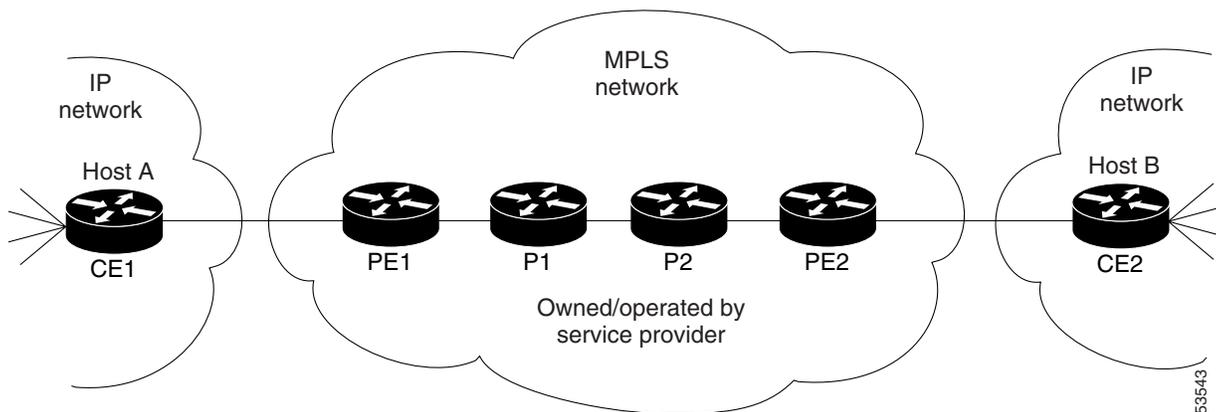
**Table 3** Cisco Express Forwarding Configuration Commands

| For This Device ...      | Enter This Command ...          |
|--------------------------|---------------------------------|
| Cisco 7200 series router | <code>ip cef</code>             |
| Cisco 7500 series router | <code>ip cef distributed</code> |

## Optionally Setting the MPLS Experimental Field Value

[Figure 1](#) is a representation of an MPLS service provider network that connects two hosts of a customer's IP network. This network topology provides a framework for this section (and subsequent sections) in which the configuration tasks associated with using the MPLS QoS multi-VC mode feature are described.

**Figure 1** MPLS Network Connecting Hosts in an IP Network



The ability to optionally set the MPLS experimental (EXP) field of the label header upon entry of a customer IP packet into an MPLS network has no direct connection to the MPLS QoS multi-VC mode feature per se. However, if the service provider wants to preserve the IP precedence value in the IP type-of-service (TOS) byte in the header of an incoming IP packet for any reason (such as for managing queues or selecting LVCs based on the value of the EXP field), the ability to manipulate the EXP field provides such flexibility.

By default, the IP precedence field in the header of incoming IP packets is copied into the MPLS EXP field in the label header upon entry of IP packets into the service provider's MPLS network. This default action enables IP packets to be differentiated into queues (for congestion management purposes) and to

be directed to appropriate LVCs (for transmission of customer data through the MPLS network). Thus, if the IP precedence field is set, either on the edge router in the MPLS network or on some other upstream device, the incoming customer IP packets are assured of using the appropriate LVCs for data transport through the service provider network.

Optionally, you can set the MPLS EXP field value in customer IP packets arriving at the provider edge router (the PE1 ingress label switching router in [Figure 1](#)) by means of modular QoS CLI commands or CAR commands executed on that edge router. This action establishes a specified level of service for customer data traversing the service provider's MPLS network, while, at the same time, preserving the value of the IP precedence field in the incoming customer IP packets.

By assigning any one of eight different values to the EXP field (see the [“Classifying Packets”](#) section), you can mark each incoming IP packet for transport through the service provider network according to such packet attributes as packet rate and packet type.

By classifying packets, you can establish the relative priority of packets for discard purposes if congestion is experienced within the service provider network. The [“Packet Prioritization”](#) section discusses in more detail the attributes used in determining the relative priority of packets for congestion management purposes.

## Classifying Packets

To classify IP packets, the PE1 ingress label switching router (LSR) in the service provider network (see [Figure 1](#)) must be appropriately configured. When so configured, customer IP packets received at the ingress router are propagated through the service provider network as MPLS packets.

You can use either of two methods to classify IP packets at the ingress LSR in the service provider's MPLS network:

- Modular QoS CLI (a newer and more flexible method)—Use this method if you *do not* want to consider the rate of receipt of IP packets at the ingress LSR.
- CAR—Use this method if you *do* want to consider the rate of receipt of IP packets at the ingress LSR.
  - If a packet conforms to the service level agreement (SLA) between the service provider and the customer (that is, if the incoming IP packet is “in-rate”), the service provider gives the packet preferential treatment during transit through the MPLS network under congestion conditions.
  - If a packet does not conform to the SLA (that is, if the incoming IP packet is “out-of-rate”) and congestion occurs in the service provider network, the service provider can discard the packet altogether or give the packet less preferential treatment relative to other network traffic.

## Packet Prioritization

During Step 1 of the configuration process (described in the [“Using Modular QoS CLI to Configure Ingress Label Switching Router”](#) section and the [“Using CAR to Configure Ingress Label Switching Router”](#) section), customer IP packets are classified according to the following attributes:

- Source address
- Destination address
- Port
- Protocol identification
- Class of service field

Based on one or more of the above attributes, packets can be identified as Voice over IP (VoIP) traffic or File Transfer Protocol (FTP) traffic. This packet classification/marketing process determines the packet's relative priority during transit through the service provider network, particularly amidst network congestion conditions.

The SLA in effect for each customer of the service provider network specifies how much bandwidth the service provider agrees to make available to each customer. To comply with the agreement, the customer must not exceed a specified traffic rate. Packets are considered to be either in-rate or out-of-rate per the SLA. Thus, during periods of congestion in the service provider network, the potential exists for out-of-rate packets to be discarded more aggressively.

## Using Modular QoS CLI to Configure Ingress Label Switching Router

To use the modular QoS CLI to configure the ingress LSR (PE1 in [Figure 1](#)) appropriately for multi-VC mode functionality, perform the following steps:

- 
- Step 1** Configure a class map to classify IP packets according to their IP precedence.
  - Step 2** Configure a policy map to mark MPLS packets (that is, to write their classification into the MPLS EXP field).
  - Step 3** Configure the input interface of the ingress router to attach the service policy.
- 

The following sections describe in detail how to accomplish the generalized steps outlined above.

### Configuring a Class Map to Classify IP Packets

To configure a class map on the ingress LSR, use the following commands:

|               | Command                                                | Purpose                                                                 |
|---------------|--------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>class-map</b> <i>class-map name</i> | Specifies the class map to which incoming IP packets will be matched.   |
| <b>Step 2</b> | Router(config-c-map)# <b>match</b> <i>criteria</i>     | Specifies the packet characteristics that will be matched to the class. |
| <b>Step 3</b> | Router(config-c-map)# <b>end</b>                       | Exits the class map configuration mode.                                 |

In the following example, all packets that contain IP precedence 4 are matched by the class-map name IP\_prec4:

```
Router(config)# class-map IP_prec4
Router(config-c-map)# match ip precedence 4
Router(config-c-map)# end
```

## Configuring a Policy Map to Mark MPLS EXP Field

To configure a policy map to mark the MPLS EXP field in IP packets arriving at the ingress LSR, use the following commands:

|        | Command                                                           | Purpose                                                                                                                |
|--------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>policy-map</b> <i>policy-map name</i>          | Creates a policy map that can be attached to one or more ingress interfaces to specify a service policy.               |
| Step 2 | Router(config-p-map)# <b>class</b> <i>class-map name</i>          | Specifies the name of the class map previously designated by means of the <b>class-map</b> command in the table above. |
| Step 3 | Router(config-p-map-c)# <b>set mpls experimental</b> <i>value</i> | Designates the value to which the MPLS EXP bits will be set if the incoming IP packets match the specified policy map. |
| Step 4 | Router(config-p-map-c)# <b>end</b>                                | Exits the policy map configuration mode.                                                                               |

In the following example, the MPLS EXP field of each IP packet that matches class-map *IP\_prec4* is set to a value of 5:

```
Router(config)# policy-map set_experimental_5
Router(config-p-map)# class IP_prec4
Router(config-p-map-c)# set mpls experimental 5
Router(config-p-map-c)# end
```

## Configuring Input Interface to Attach Service Policy

To configure the input interface of the ingress LSR to attach the service policy, use the following steps:

|        | Command                                                               | Purpose                                                                         |
|--------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <i>name</i>                          | Designates the input interface.                                                 |
| Step 2 | Router(config-if)# <b>service-policy input</b> <i>policy-map name</i> | Attaches the specified policy map to the input interface of the ingress device. |
| Step 3 | Router(config-if)# <b>end</b>                                         | Exits the interface configuration mode.                                         |

In the following example, the service policy *set\_experimental\_5* is attached to the specified Ethernet input interface (*et 1/0/0*):

```
Router(config)# interface et 1/0/0
Router(config-if)# service-policy input set_experimental_5
Router(config-if)# end
```

## Using CAR to Configure Ingress Label Switching Router

To use CAR to configure the ingress LSR (PE1 in [Figure 1](#)) for multi-VC mode functionality, perform the following steps:

- 
- Step 1** Configure an IP rate-limit access list for classifying IP packets according to their IP precedence.
  - Step 2** Configure a rate-limit on an input interface to mark the MPLS packets (to write the packet's classification into the MPLS EXP field).
- 

The following sections describe in detail how to accomplish the generalized steps outlined above.

### Configuring Rate-Limit Access List for Classifying IP Packets

To configure a rate-limit access list for classifying IP packets arriving at the ingress LSR, perform the following steps:

|               | Command                                                                      | Purpose                               |
|---------------|------------------------------------------------------------------------------|---------------------------------------|
| <b>Step 1</b> | Router(config)# <b>access-list rate-limit</b><br><i>acl-index precedence</i> | Specifies the criteria to be matched. |
| <b>Step 2</b> | Router(config)# <b>end</b>                                                   | Exits the global configuration mode.  |

In the following example, all packets containing IP precedence value 4 are matched by the rate-limit access list 24:

```
Router(config)# access-list rate-limit 24 4
Router(config)# end
```

### Configuring Rate-Limit on Input Interface to Mark MPLS Packets

To configure a rate-limit on an input interface to mark MPLS packets on the ingress LSR, perform the following steps:

|               | Command                                                                                                                                                                                                                                                                            | Purpose                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface</b> <i>name</i>                                                                                                                                                                                                                                       | Designates the input interface.                                          |
| <b>Step 2</b> | Router(config-if)# <b>rate-limit input</b><br>[ <b>access-group</b> [ <b>rate-limit</b> ] <i>acl-index</i> ] <i>bps</i><br><i>burst-normal burst-max conform-action</i><br><b>set-mpls-exp-transmit</b> <i>exp</i> <b>exceed-action</b><br><b>set-mpls-exp-transmit</b> <i>exp</i> | Specifies the actions to be taken on IP packets during label imposition. |
| <b>Step 3</b> | Router(config-if)# <b>end</b>                                                                                                                                                                                                                                                      | Exits the interface configuration mode.                                  |

In the following example, the MPLS EXP field is set to 4 on output of packets if input IP packets match the access-list and conform to the packet rate. The MPLS EXP field is set to 0 if packets match access list 24 and exceed the input rate.

```
Router(config)# interface et 1/0/0
Router(config-if)# rate-limit input access-group rate-limit 24 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
Router(config-if)# end
```

## Configuring Class of Service for IP Packets on Output

The class of service for IP packets exiting the service provider network is determined by information carried in the header of each IP packet. For configuration details, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

## Configuring MPLS QoS in Core of ATM Network

The following sections describe how to configure MPLS QoS in the core of an ATM network.

### Configuring Multi-VC Mode in MPLS-Enabled Network

To configure multi-VC mode in an MPLS-enabled network, issue the following commands:

|               | Command                                              | Purpose                                                                                                                                    |
|---------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface</b> type number mpls    | Configures an ATM MPLS subinterface.                                                                                                       |
| <b>Step 2</b> | Router(config-subif)# <b>ip unnumbered Loopback0</b> | Assigns an IP address to the subinterface.                                                                                                 |
| <b>Step 3</b> | Router(config-subif)# <b>mpls atm multi-vc</b>       | Enables ATM multi-VC mode on the subinterface. This step results in the creation of the default QoS map shown in <a href="#">Table 4</a> . |
| <b>Step 4</b> | Router(config-subif)# <b>mpls ip</b>                 | Enables MPLS on the ATM subinterface.                                                                                                      |
| <b>Step 5</b> | Router(config-subif)# <b>mpls label-protocol ldp</b> | Configures LDP, rather than TDP, as the label distribution protocol.                                                                       |

If you do not configure a QoS map and apply it to a destination by means of a prefix map, enabling the ATM multi-VC mode on a subinterface (as done in Step 3 above) results in the creation of the default QoS map shown in [Table 4](#). This default action creates four LVCs (Available, Standard, Premium, and Control) for each destination, and the two least significant bits of the EXP field determine the LVC to which the IP packets will be directed.

**Table 4** Default QoS Map

| EXP Field Value | LVC       |
|-----------------|-----------|
| 0               | Available |
| 1               | Standard  |
| 2               | Premium   |
| 3               | Control   |
| 4               | Available |
| 5               | Standard  |
| 6               | Premium   |
| 7               | Control   |

## Configuring Multi-VCs Using the QoS-Map Function

If you choose to not use the default QoS map for configuring label VCs, you can configure fewer label VCs by using the QoS map function. To use this function, issue the following commands:

|        | Command                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>mpls cos-map</b> <i>cos-map number</i>                            | Creates a QoS map.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | Router(config-tag-cos-map)# <b>class 1 premium</b>                                   | Enters the cos-map submode and maps traffic classes to LVCs.<br>The QoS map created by this step assigns class 1 traffic (standard) to share the same LVC as class 2 traffic (premium).<br>The default values for assigning traffic classes to the QoS map range from 0 to 3, as follows:<br>Class 0—Available<br>Class 1—Standard<br>Class 2—Premium<br>Class 3—Control<br>The class of a packet is determined by the two least significant bits of the EXP field in the packet header. |
| Step 3 | Router(config-tag-cos-map)# <b>exit</b>                                              | Exits the MPLS QoS map submode.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | Router(config)# <b>access-list</b> <i>access-list-number permit destination</i>      | Creates an access list to control traffic going to the specified destination address.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 5 | Router(config)# <b>mpls prefix-map</b> <i>prefix-map access-list cos-map cos-map</i> | Configures the router to use a specified QoS map when an MPLS destination prefix matches the specified access list.                                                                                                                                                                                                                                                                                                                                                                      |

## Configuring Queueing Functions on Router Output Interfaces

### Configuring CBWFQ on Cisco 7200/7500 Series and Cisco MGX RPM-PR Router Interfaces

To configure class-based weighted fair queueing (CBWFQ) functionality on a Cisco 7200 or 7500 series router interface or on the router interface of a Cisco MGX Route Processor Module (RPM-PR) in the Cisco MGX 8850 or 8950 switch, issue the following commands:

|        | Command                                                       | Purpose                                                                                              |
|--------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>class-map</b> <i>class-map-name</i>        | Creates a class-map.                                                                                 |
| Step 2 | Router(config-cmap)# <b>match mpls experimental 5</b>         | Enters the class-map submode and determines what packets this class-map should match on.             |
| Step 3 | Router(config-cmap)# <b>policy-map</b> <i>policy-map-name</i> | Creates a policy-map.                                                                                |
| Step 4 | Router(config-pmap)# <b>class</b> <i>class-map-name</i>       | Calls the previously created class-map.                                                              |
| Step 5 | Router(config-pmap-c)# <b>bandwidth percent 35</b>            | Configures the policy-map to have CBWFQ acting on packets matching the previously created class-map. |

|        | Command                                                                | Purpose                                  |
|--------|------------------------------------------------------------------------|------------------------------------------|
| Step 6 | Router(config)# <b>interface</b> <i>type number</i>                    | Specifies the interface type and number. |
| Step 7 | Router(config-if)# <b>service-policy output</b> <i>policy-map-name</i> | Assigns the policy-map on the interface. |

## Configuring WRED on Cisco 7200/7500 Series or Cisco MGX RPM-PR Router Interfaces

To configure weighted random early detection (WRED) functionality on a Cisco 7200 or 7500 series router interface or on the router interface of a Cisco MGX Route Processor Module (RPM-PR) in the Cisco MGX 8850 or 8950 switch, issue the following commands:

|        | Command                                                                | Purpose                                                                                              |
|--------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>class-map</b> <i>class-map-name</i>                 | Creates a class-map.                                                                                 |
| Step 2 | Router(config-cmap)# <b>match mpls experimental 5</b>                  | Enters the class-map submode and determines what packets this class-map should match on.             |
| Step 3 | Router(config-cmap)# <b>policy-map</b> <i>policy-map-name</i>          | Creates a policy-map.                                                                                |
| Step 4 | Router(config-pmap)# <b>class</b> <i>class-map-name</i>                | Calls the previously created class-map.                                                              |
| Step 5 | Router(config-pmap-c)# <b>bandwidth percent 35</b>                     | Configures the policy-map to have CBWFQ acting on packets matching the previously created class-map. |
| Step 6 | Router(config-pmap-c)# <b>random-detect</b>                            | Configures the policy-map to have WRED acting on packets matching the class-map.                     |
| Step 7 | Router(config)# <b>interface</b> <i>type number</i>                    | Specifies the interface type and number.                                                             |
| Step 8 | Router(config-if)# <b>service-policy output</b> <i>policy-map-name</i> | Assigns the policy-map on the interface.                                                             |

## Setting the ATM-CLP Bit on PA-A3 Interfaces

To set the atm-clp bit in ATM cells exiting from a PA-A3 (Enhanced ATM Port Adapter) interface incorporated into a Cisco 7200 or Cisco 7500 router, issue the following commands on the router.

|        | Command                                                                | Purpose                                                                                        |
|--------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>class-map</b> <i>class-map-name</i>                 | Creates a class-map.                                                                           |
| Step 2 | Router(config-cmap)# <b>match mpls experimental 5</b>                  | Enters the class-map submode and determines what packets this class-map should match on.       |
| Step 3 | Router(config-cmap)# <b>policy-map</b> <i>policy-map-name</i>          | Creates a policy-map.                                                                          |
| Step 4 | Router(config-pmap)# <b>class</b> <i>class-map-name</i>                | Calls the previously created class-map.                                                        |
| Step 5 | Router(config-pmap-c)# <b>set atm-clp</b>                              | Causes all MPLS packets matching this class to have the CLP bit set in the outgoing ATM cells. |
| Step 6 | Router(config)# <b>interface</b> <i>type number</i>                    | Specifies the interface type and number.                                                       |
| Step 7 | Router(config-if)# <b>service-policy output</b> <i>policy-map-name</i> | Assigns the policy-map on the interface.                                                       |

## Verifying QoS Configuration on ATM Interfaces

To verify MPLS QoS configuration on ATM interfaces, use the following commands:

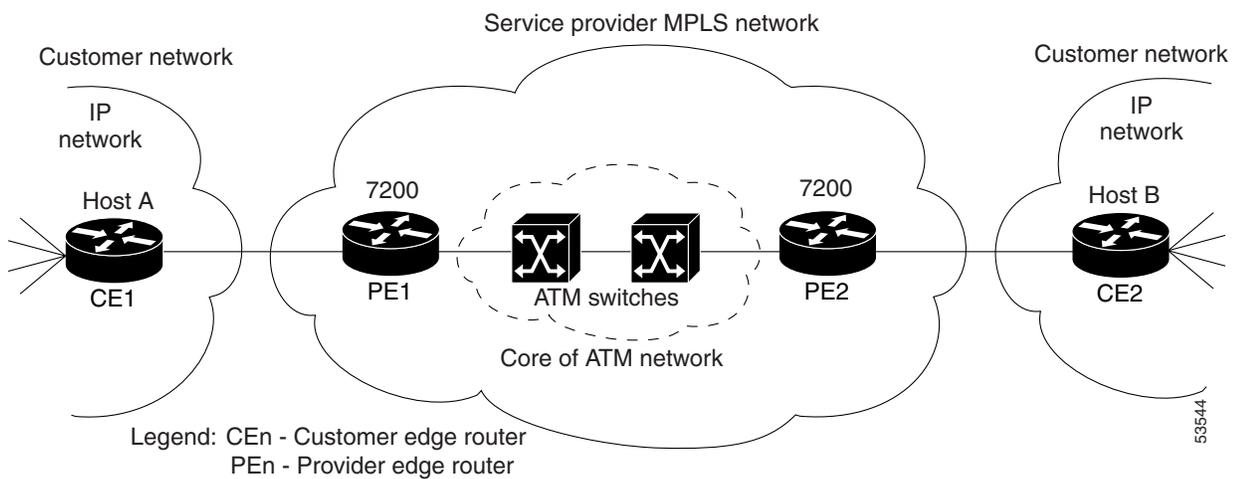
|               | <b>Command</b>                                        | <b>Purpose</b>                                                        |
|---------------|-------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Step 1</b> | Router# <b>show mpls interfaces</b> <i>interfaces</i> | Displays detailed information about label switching interfaces.       |
| <b>Step 2</b> | Router# <b>show mpls cos-map</b>                      | Displays the QoS map used to assign LVCs.                             |
| <b>Step 3</b> | Router# <b>show mpls prefix-map</b>                   | Displays the prefix map used to assign a QoS map to network prefixes. |

# Configuration Examples

Figure 2 is a sample network topology for which MPLS QoS multi-VC mode functionality has been configured for Cisco 7200 series routers in a customer IP network and a service provider MPLS network. IP and MPLS configuration examples for the following network components are provided in this section:

- [Running IP on Customer Edge Router 1 \(CE1\)](#)
- [Running IP on Customer Edge Router 2 \(CE2\)](#)
- [Running MPLS on Provider Edge Router 1 \(PE1\)](#)
- [Running MPLS on Provider Edge Router 2 \(PE2\)](#)

**Figure 2** Configuring MPLS QoS Multi-VC Mode Functionality on IP and MPLS Network Devices



## Running IP on Customer Edge Router 1 (CE1)

The following sample output shows how IP has been configured to run on customer edge router 1 (CE1) shown in Figure 2:

```
interface Loopback0
 ip address 11.11.11.11 255.255.255.255
!
interface POS3/2
 ip address 31.0.0.1 255.0.0.0
 no ip directed-broadcast
 crc 16
 clock source internal
!
router bgp 101
 no synchronization
 bgp log-neighbor-changes
 network 11.11.11.11 mask 255.255.255.255
 network 31.0.0.0
 redistribute connected
 redistribute static
 neighbor 31.0.0.2 remote-as 100
 neighbor 31.0.0.2 advertisement-interval 5
 no auto-summary
```

## Running IP on Customer Edge Router 2 (CE2)

The following sample output shows how IP has been configured to run on the customer edge router 2 (CE2) shown in [Figure 2](#):

```
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface POS3/2
ip address 31.0.0.2 255.0.0.0
no ip directed-broadcast
 crc 16
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 redistribute bgp 102
 passive-interface POS3/2
 passive-interface POS5/0
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 102
 no synchronization
 bgp log-neighbor-changes
 network 10.0.0.0
 network 31.0.0.0
 redistribute connected
 redistribute static
 redistribute ospf 100
 neighbor 31.0.0.1 remote-as 100
 neighbor 31.0.0.1 advertisement-interval 5
 no auto-summary
```

## Running MPLS on Provider Edge Router 1 (PE1)

The following sample output shows how MPLS has been configured to run on provider edge router 1 (PE1) shown in [Figure 2](#):

```
ip cef
!
class-map match-all exp0
 match mpls experimental 0 4
class-map match-all exp1
 match mpls experimental 1 5
class-map match-all exp2
 match mpls experimental 2 6
class-map match-all exp3
 match mpls experimental 3 7
class-map match-all acl101
 match access-group 101
class-map match-all acl102
 match access-group 102
!
policy-map atm_output
 class exp0
 bandwidth percent 10
 class exp1
 bandwidth percent 25
 class exp2
 bandwidth percent 20
 class exp3
```

```

 bandwidth percent 20
 !
 policy-map input_int
 class acl101
 police cir 64000 bc 2000 conform-action set-mpls-exp-transmit 2 exceed-action
 set-mpls-exp-transmit 1
 class acl102
 police cir 32000 bc 1500 conform-action set-mpls-exp-transmit 3 exceed-action drop
 !
 ip vrf test1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 100:2
 no ip dhcp-client network-discovery
 no mgcp timer receive-rtcp
 call rsvp-sync
 !
 interface Loopback0
 ip address 12.12.12.12 255.255.255.255
 !
 interface ATM1/0.1 tag-switching
 ip unnumbered Loopback0
 service-policy output atm_output
 no ip mroute-cache
 tag-switching atm multi-vc
 tag-switching atm vpi 2-5
 tag-switching ip
 !
 interface POS 6/0
 service-policy input input_int
 ip vrf forwarding test1
 ip address 31.0.0.2 255.0.0.0
 clock source internal
 !
 router ospf 100
 log-adjacency-changes
 redistribute connected subnets
 passive-interface POS6/0
 network 12.0.0.0 0.255.255.255 area 100
 !
 router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 redistribute static
 neighbor 14.14.14.14 remote-as 100
 neighbor 14.14.14.14 update-source Loopback0
 !
 address-family ipv4 vrf test1
 redistribute connected
 neighbor 30.0.0.1 remote-as 101
 neighbor 30.0.0.1 activate
 neighbor 30.0.0.1 advertisement-interval 5
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 14.14.14.14 activate
 neighbor 14.14.14.14 send-community extended
 bgp scan-time import 5
 exit-address-family
 !

```

```
access-list 101 permit ip host 11.11.11.11 any
access-list 102 permit ip host 31.0.0.1 any
```

## Running MPLS on Provider Edge Router 2 (PE2)

The following sample output shows how MPLS has been configured to run on provider edge router 2 (PE2) shown in [Figure 2](#):

```
ip cef
!
class-map match-all exp0
 match mpls experimental 0 4
class-map match-all exp1
 match mpls experimental 1 5
class-map match-all exp2
 match mpls experimental 2 6
class-map match-all exp3
 match mpls experimental 3 7
class-map match-all acl101
 match access-group 101
class-map match-all acl102
 match access-group 102
!
policy-map atm_output
 class exp0
 bandwidth percent 10
 class exp1
 bandwidth percent 25
 class exp2
 bandwidth percent 20
 class exp3
 bandwidth percent 20
!
policy-map input_int
 class acl101
 police cir 64000 bc 2000 conform-action set-mpls-exp-transmit 2 exceed-action
 set-mpls-exp-transmit 1
 class acl102
 police cir 32000 bc 1500 conform-action set-mpls-exp-transmit 3 exceed-action drop
!
ip vrf test2
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 route-target import 100:1
no ip dhcp-client network-discovery
no mgcp timer receive-rtcp
call rsvp-sync
!
interface Loopback0
 ip address 14.14.14.14 255.255.255.255
!
interface ATM5/0.1 tag-switching
 ip unnumbered Loopback0
 service-policy output atm_output
 no ip mroute-cache
 tag-switching atm multi-vc
 tag-switching atm vpi 2-5
 tag-switching ip
!
interface POS6/0
 service-policy input input_int
```

```
 ip vrf forwarding test2
 ip address 31.0.0.1 255.0.0.0
 clock source internal
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 redistribute connected subnets
 passive-interface POS6/0
 network 14.0.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 redistribute static
 neighbor 12.12.12.12 remote-as 100
 neighbor 12.12.12.12 update-source Loopback0
!
 address-family ipv4 vrf test2
 redistribute connected
 neighbor 31.0.0.2 remote-as 102
 neighbor 31.0.0.2 activate
 neighbor 31.0.0.2 advertisement-interval 5
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor 12.12.12.12 activate
 neighbor 12.12.12.12 send-community extended
 bgp scan-time import 5
 exit-address-family
!
access-list 101 permit ip host 10.10.10.10 any
access-list 102 permit ip host 31.0.0.2 any
```

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **access-list rate-limit**
- **debug mpls atm-cos**
- **match mpls experimental**
- **mpls atm multi-vc**
- **mpls cos-map**
- **mpls prefix-map**
- **rate-limit**
- **set atm-clp**
- **set mpls experimental**
- **show mpls cos-map**
- **show mpls prefix-map**

# Glossary

**ATM edge LSR**—A router that is connected to the ATM-LSR cloud through an LSC-ATM interface. The ATM edge LSR adds labels to unlabeled packets and strips labels from labeled packets.

**ATM-LSR**—A label switch router with a number of LSC-ATM interfaces. The router forwards ATM cells among these interfaces using labels carried in the VPI/VCI field.

**CAR**—Committed access rate (packet classification). CAR is the main feature supporting packet classification. CAR uses the type of service (ToS) bits in the IP header to classify packets. You can use the CAR classification commands to classify or reclassify a packet.

**Class-based weighted fair queuing (CBWFQ)**—CBWFQ extends standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria which include protocols, access control lists (ACLs), and input interfaces. Packets satisfying match criteria for a class constitute the traffic for that class. A queue is reserved for each class, and the traffic belonging to a class is directed to the queue for that class.

**IP precedence**—A 3-bit value in the ToS byte that is used for assigning precedence to IP packets.

**label**—A short, fixed-length construct that tells switching nodes how to forward data (packets or cells) in a network.

**label-controlled ATM interface (LC-ATM interface)**—An interface on a router or switch that uses label distribution procedures to negotiate label VCs.

**label edge router (LER)**—A router that performs label imposition at the point of ingress in a network.

**label imposition**—The process of adding the first label on a packet.

**label switch**—A node that forwards units of data (packets or cells) on the basis of labels carried in the packets or cells.

**label switch path (LSP)**—An LSP results from a series of hops (Router 0...Router n) through which a packet travels from R0 to Rn by means of label switching mechanisms. A label-switched path can be determined dynamically (based on normal routing mechanisms), or it can be defined explicitly.

**label-switched path (LSP) tunnel**—A configured connection between two routers, in which label switching techniques are used for packet forwarding.

**label switching router (LSR)**—A Layer 3 router that forwards packets based on the value of a label encapsulated in each packet.

**label VC (LVC)**—An ATM virtual circuit that is set up through ATM LSR label distribution procedures.

**LBR**—Label bit rate. A service category defined for label-VC traffic. Link and per-VC bandwidth sharing can be controlled by relative bandwidth configuration at the edge of the network and each switch along a label-VC. No ATM traffic-related parameters are specified.

**LDP**—Label Distribution Protocol. The protocol used to distribute label bindings to LSRs.

**LFIB**—Label forwarding information base. The data structure used by switching functions to switch labeled packets.

**LIB**—Label information base. A database used by an LSR to store labels learned from other LSRs, as well as labels assigned by the local LSR.

**MPLS**—Multiprotocol Label Switching. An emerging industry standard that defines support for MPLS forwarding of packets along normally routed paths (sometimes called MPLS hop-by-hop forwarding).

**QoS**—Quality of service. A feature that provides scalable, differentiated types of service across an MPLS network.

**RED**—Random early detection. A congestion avoidance algorithm in which a small percentage of packets are dropped automatically when congestion is detected in the network and before the queue in question overflows completely.

**ToS bits**—Type of service bits. A byte in the IPv4 packet header.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been applied.

**traffic engineering tunnel**—A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; the tunnel is used to direct traffic over a path different from the one that Layer 3 routing would otherwise cause the tunnel to take.

**VPN**—Virtual private network. Enables IP traffic to use tunneling to transport data securely over a public TCP/IP network.

**WRED**—Weighted random early detection. A variant of RED in which the probability of a packet being dropped depends on either its IP precedence, CAR marking, or MPLS class of service (as well as other factors in the RED algorithm).

**WFQ**—Weighted fair queuing. A queue management algorithm that provides a certain fraction of link bandwidth to each of several queues, based on a relative bandwidth applied to each of the queues.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



**Any Transport over MPLS (AToM)**





# Any Transport over MPLS

---

**First Published: January 1, 2001**

**Last Updated: December 17, 2007**

Any Transport over MPLS (AToM) transports data link layer (Layer 2) packets over a Multiprotocol Label Switching (MPLS) backbone. AToM enables service providers to connect customer sites with existing Layer 2 networks by using a single, integrated, packet-based network infrastructure—a Cisco MPLS network. Instead of using separate networks with network management environments, service providers can deliver Layer 2 connections over an MPLS backbone. AToM provides a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network core.

AToM supports the following like-to-like transport types:

- ATM Adaptation Layer Type-5 (AAL5) over MPLS
- ATM Cell Relay over MPLS
- Ethernet over MPLS (VLAN and port modes)
- Frame Relay over MPLS
- PPP over MPLS
- High-Level Data Link Control (HDLC) over MPLS

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Any Transport over MPLS”](#) section on page 86.

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for Any Transport over MPLS, page 2](#)
- [Restrictions for Any Transport over MPLS, page 3](#)
- [Information About Any Transport over MPLS, page 5](#)
- [How to Configure Any Transport over MPLS, page 14](#)
- [Configuration Examples for Any Transport over MPLS, page 76](#)
- [Additional References, page 84](#)
- [Command Reference, page 86](#)
- [Feature Information for Any Transport over MPLS, page 86](#)

## Prerequisites for Any Transport over MPLS

Before configuring AToM, ensure that the network is configured as follows:

- Configure IP routing in the core so that the provider edge (PE) routers can reach each other via IP.
- Configure MPLS in the core so that a label-switched path (LSP) exists between the PE routers.
- Enable Cisco Express Forwarding or distributed Cisco Express Forwarding before configuring any Layer 2 circuits.
- Configure a loopback interface for originating and terminating Layer 2 traffic. Make sure the PE routers can access the other router's loopback interface. Note that the loopback interface is not needed in all cases. For example, tunnel selection does not need a loopback interface when AToM is directly mapped to a traffic engineering (TE) tunnel.
- AToM is supported on the Cisco 7200 and 7500 series routers. For details on supported hardware, see the following documents:
  - [Cross-Platform Release Notes for Cisco IOS Release 12.0S](#)
  - [Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 2: Platform-Specific Information](#)
- AToM is supported on the Cisco 7600 routers. For details on supported shared port adapters and line cards, see the following documents:
  - [Supported Hardware for Cisco 7600 Series Routers with Release 12.2SR](#)
  - [Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers](#)
- The Cisco 7600 router has platform-specific instructions for configuring some AToM features. Platform-specific configuration information is included in the following documents:
  - The “Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching” module of the [Cisco 7600 Series Cisco IOS Software Configuration Guide](#), Release 12.2SR
  - The “Configuring Multiprotocol Label Switching on the Optical Services Modules” module of the [OSM Configuration Note](#), Release 12.2SR
  - The “Configuring Multiprotocol Label Switching on FlexWAN and Enhanced FlexWAN Modules” module of the [Cisco 7600 Series Router Module Configuration Notes](#)
  - The “Configuring Any Transport over MPLS on a SIP” section of the [Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide](#)

- The “Configuring AToM VP Cell Mode Relay Support” section of the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*
- The *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*
- AToM is supported on the Cisco 10000 series routers. For details on supported hardware, see the “Configuring Any Transport over MPLS” section of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*.
- The Cisco 10000 series router has platform-specific instructions for configuring some AToM features. Platform-specific configuration information is contained in the “Configuring Any Transport over MPLS” section of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*.
- AToM is supported on the Cisco 12000 series routers. For information about hardware requirements, see the *Cross-Platform Release Notes for Cisco IOS Release 12.0S*.

## Restrictions for Any Transport over MPLS

The following general restrictions pertain to all transport types under AToM:

- Address format: Configure the Label Distribution Protocol (LDP) router ID on all PE routers to be a loopback address with a /32 mask. Otherwise, some configurations might not function properly.
- Layer 2 virtual private networks (L2VPN) features (AToM and Layer 2 Tunnel Protocol Version 3 (L2TPv3)) are not supported on an ATM interface.
- Distributed Cisco Express Forwarding is the only forwarding model supported on the Cisco 12000 series routers and is enabled by default. Disabling distributed Cisco Express Forwarding on the Cisco 12000 series routers disables forwarding.
- Distributed Cisco Express Forwarding mode is supported on the Cisco 7500 series routers for Frame Relay, HDLC, and PPP. In distributed Cisco Express Forwarding mode, the switching process occurs on the Versatile Interface Processors (VIPs) that support switching. When distributed Cisco Express Forwarding is enabled, VIP port adapters maintain identical copies of the Forwarding Information Base (FIB) and adjacency tables. The port adapters perform the express forwarding between port adapters, relieving the Route Switch Processor (RSP) from performing the switching. Distributed Cisco Express Forwarding uses an interprocess communications (IPC) mechanism to ensure synchronization of FIBs and adjacency tables between the RSP and port adapters.

**The following restrictions pertain to ATM Cell Relay over MPLS:**

- **For ATM Cell Relay over MPLS**, if you have TE tunnels running between the PE routers, you must enable LDP on the tunnel interfaces.
- **Configuring ATM Relay over MPLS with the Cisco 12000 Series Router engine 2 8-port OC-3 STM-1 ATM line card:** In Cisco IOS Release 12.0(25)S, there were special instructions for configuring ATM cell relay on the Cisco 12000 series router with an engine 2 8-port OC-3 STM-1 ATM line card. The special configuration instructions are no longer needed. You no longer need to use the **atm mode cell-relay** command.

In Cisco IOS Release 12.0(25)S, when you configured the Cisco 12000 series 8-port OC-3 STM-1 ATM line card for ATM Cell Relay over MPLS, two ports were reserved. That is no longer true. Only one port is reserved now.

In addition, in Cisco IOS Release 12.0(25)S, if you configured an 8-port OC-3 STM-1 ATM port for ATM AAL5 over MPLS and then configured ATM single cell relay over MPLS on that port, the VCs and VPs for AAL5 on the port and its corresponding port were removed. Starting in Cisco IOS Release 12.0(26)S, this behavior no longer occurs. ATM AAL5 over MPLS and ATM single cell

relay over MPLS are supported on the same port. The Cisco 12000 series 8-port OC-3 STM-1 ATM line cards now support, by default, the ATM single cell relay over MPLS feature in both VP and VC modes and ATM AAL5 over MPLS on the same port.

- The F4 end-to-end OAM cells are transparently transported along with the ATM cells. When a permanent virtual path (PVP) or PVC is down on one PE router, the label associated with that PVP or PVC is withdrawn. Subsequently, the peer PE router detects the label withdrawal and sends an F4 AIS/RDI signal to its corresponding CE router. The PVP or PVC on the peer PE router remains in the up state.

The following restrictions pertain to the Ethernet over MPLS feature:

- Ethernet over MPLS supports VLAN packets that conform to the IEEE 802.1Q standard. The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. The Inter-Switch Link (ISL) protocol is not supported between the PE and CE routers.
- The AToM control word is supported. However, if the peer PE does not support a control word, the control word is disabled. This negotiation is done by LDP label binding.
- Ethernet packets with hardware-level cyclic redundancy check (CRC) errors, framing errors, and runt packets are discarded on input.
- In Cisco IOS Release 12.2(25)S, the behavior of the **mpls mtu** command changed. If the interface MTU is less than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).



#### Caution

---

Although you can set the MPLS MTU to a value greater than the interface MTU, set the MPLS MTU less than or equal to the interface MTU to prevent data corruption, dropped packets, and high CPU rates..

---

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and the interface MTU is 1500 bytes, the MPLS MTU range is 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S from an earlier release and you have an MPLS MTU setting that does not conform to these guidelines, the command is rejected. See the [“Maximum Transmission Unit Guidelines for Estimating Packet Size”](#) section on page 7 for more information.

The following restrictions pertain to the Frame Relay over MPLS feature:

- Frame Relay traffic shaping is not supported with AToM switched VCs.
- If you configure Frame Relay over MPLS on the Cisco 12000 series router and the core-facing interface is an engine 4 or 4+ line card and the edge-facing interface is an engine 0 or 2 line card, then the BECN, FECN, control word (CW), and DE bit information is stripped from the PVC.

# Information About Any Transport over MPLS

To configure AToM, you must understand the following concepts:

- [How AToM Transports Layer 2 Packets, page 5](#)
- [AToM Configuration Commands Prior to Cisco IOS Release 12.0\(25\)S, page 6](#)
- [Benefits of AToM, page 6](#)
- [MPLS Traffic Engineering Fast Reroute, page 6](#)
- [Maximum Transmission Unit Guidelines for Estimating Packet Size, page 7](#)
- [Frame Relay over MPLS and DTE, DCE, and NNI Connections, page 9](#)
- [QoS Features Supported with AToM, page 11](#)

## How AToM Transports Layer 2 Packets

AToM encapsulates Layer 2 frames at the ingress PE and sends them to a corresponding PE at the other end of a pseudowire, which is a connection between the two PE routers. The egress PE removes the encapsulation and sends out the Layer 2 frame.

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. You set up the connection, called a pseudowire, between the routers. You specify the following information on each PE router:

- The type of Layer 2 data that will be transported across the pseudowire, such as Ethernet, Frame Relay, or ATM
- The IP address of the loopback interface of the peer PE router, which enables the PE routers to communicate
- A unique combination of peer PE IP address and VC ID that identifies the pseudowire

The following example shows the basic configuration steps on a PE router that enable the transport of Layer 2 packets. Each transport type has slightly different steps.

Step 1 defines the interface or subinterface on the PE router:

```
Router# interface interface-type interface-number
```

Step 2 specifies the encapsulation type for the interface, such as dot1q:

```
Router(config-if)# encapsulation encapsulation-type
```

Step 3 does the following:

- Makes a connection to the peer PE router by specifying the LDP router ID of the peer PE router.
- Specifies a 32-bit unique identifier, called the VC ID, which is shared between the two PE routers. The combination of the peer router ID and the VC ID must be unique on the router. Two circuits cannot use the same combination of peer router ID and VC ID.
- Specifies the tunneling method used to encapsulate data in the pseudowire. AToM uses MPLS as the tunneling method.

```
Router(config-if)# xconnect peer-router-id vcid encapsulation mpls
```

As an alternative, you can set up a pseudowire class to specify the tunneling method and other characteristics. See the [“Configuring the Pseudowire Class” section on page 15](#) for more information.

## AToM Configuration Commands Prior to Cisco IOS Release 12.0(25)S

In releases of AToM previous to Cisco IOS 12.0(25)S, the command used to configure AToM circuits was **mpls l2 transport route**. This command has been replaced with the **xconnect** command.

No enhancements will be made to the **mpls l2transport route** command. Enhancements will be made to either the **xconnect** command or **pseudowire-class** command. Therefore, Cisco recommends that you use the **xconnect** command to configure AToM circuits.

Configurations from releases previous to Cisco IOS 12.0(25)S that use the **mpls l2transport route** command are still supported.

## Benefits of AToM

The following list explains some of the benefits of enabling Layer 2 packets to be sent in the MPLS network:

- The AToM product set accommodates many types of Layer 2 packets, including Ethernet and Frame Relay, across multiple Cisco router platforms, such as the Cisco 7200 and 7500 series routers. This enables the service provider to transport all types of traffic over the backbone and accommodate all types of customers.
- AToM adheres to the standards developed for transporting Layer 2 packets over MPLS. (See the “Standards” section on page 84 for the specific standards that AToM follows.) This benefits the service provider that wants to incorporate industry-standard methodologies in the network. Other Layer 2 solutions are proprietary, which can limit the service provider’s ability to expand the network and can force the service provider to use only one vendor’s equipment.
- Upgrading to AToM is transparent to the customer. Because the service provider network is separate from the customer network, the service provider can upgrade to AToM without disruption of service to the customer. The customers assume that they are using a traditional Layer 2 backbone.

## MPLS Traffic Engineering Fast Reroute

AToM can use MPLS traffic engineering (TE) tunnels with fast reroute (FRR) support. AToM VCs can be rerouted around a failed link or node at the same time as MPLS and IP prefixes.

Enabling fast reroute on AToM does not require any special commands; you can use standard fast reroute commands. At the ingress PE, an AToM tunnel is protected by fast reroute when it is routed to an FRR-protected TE tunnel. Both link and node protection are supported for AToM VCs at the ingress PE. For more information on configuring MPLS TE fast reroute, see the following document:

[\*MPLS Traffic Engineering \(TE\)—Link and Node Protection, with RSVP Hellos Support\*](#)



### Note

The AToM VC independence feature was introduced in Cisco IOS Release 12.0(31)S and enables the Cisco 12000 series router to perform fast reroute in fewer than 50 milliseconds, regardless of the number of VCs configured. In previous releases, the fast reroute time depended on the number of VCs inside the protected TE tunnel.

For the Cisco 12000 series routers, fast reroute uses three or more labels, depending on where the TE tunnel ends:

- If the TE tunnel is from a PE router to a PE router, three labels are used.

- If the TE tunnel is from a PE router to the core router, four labels are used.

Engine 0 ATM line cards support three or more labels, although performance degrades. Engine 2 Gigabit Ethernet line cards and engine 3 line cards support three or more labels and can work with the fast reroute feature.

You can issue the **debug mpls l2transport fast-reroute** command to debug fast reroute with AToM.



#### Note

This command does not display output on platforms where AToM fast reroute is implemented in the forwarding code. The command does display output on Cisco 10720 Internet router line cards and Cisco 12000 series line cards. This command does not display output for the Cisco 7500 (both Route Processor (RP) and VIP) series routers, Cisco 7200 series routers, and Cisco 12000 series RP.

In the following example, the primary link is disabled, which causes the backup tunnel (Tunnel 1) to become the primary path. In the following example, bolded output show the status of the tunnel:

```
Router# execute-on slot 3 debug mpls l2transport fast-reroute

===== Line Card (Slot 3) =====
AToM fast reroute debugging is on
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Processing TFIB FRR event for 10.4.0.1
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Finished processing TFIB FRR event for 10.4.0.1
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Processing TFIB FRR event for Tunnel41
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Finished processing TFIB FRR event for Tunnel41
Sep 16 17:58:58.342: %LINK-3-UPDOWN: Interface POS0/0, changed state to down
Sep 16 17:58:58.342: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on POS0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
Sep 16 17:58:59.342: %LINEPROTO-5-UPDOWN: Line protocol on Interface POS0/0, changed state
to down
```

## Maximum Transmission Unit Guidelines for Estimating Packet Size

The following calculation helps you determine the size of the packets traveling through the core network. You set the maximum transmission unit (MTU) on the core-facing interfaces of the P and PE routers to accommodate packets of this size. The MTU should be greater than or equal to the total bytes of the items in the following equation:

$$\text{Core MTU} \geq (\text{Edge MTU} + \text{Transport header} + \text{AToM header} + (\text{MPLS label stack} * \text{MPLS label size}))$$

The following sections describe the variables used in the equation.

### Edge MTU

The edge MTU is the MTU for the customer-facing interfaces.

### Transport Header

The Transport header depends on the transport type. [Table 1](#) lists the specific sizes of the headers.

**Table 1** Header Size of Packets

| Transport Type | Packet Size |
|----------------|-------------|
| AAL5           | 0–32 bytes  |
| Ethernet VLAN  | 18 bytes    |

**Table 1** Header Size of Packets (continued)

| Transport Type   | Packet Size                                                                                       |
|------------------|---------------------------------------------------------------------------------------------------|
| Ethernet Port    | 14 bytes                                                                                          |
| Frame Relay DLCI | 2 bytes for Cisco encapsulation, 8 bytes for Internet Engineering Task Force (IETF) encapsulation |
| HDLC             | 4 bytes                                                                                           |
| PPP              | 4 bytes                                                                                           |

**AToM Header**

The AToM header is 4 bytes (control word). The control word is optional for Ethernet, PPP, HDLC, and cell relay transport types. However, the control word is required for Frame Relay and ATM AAL5 transport types.

**MPLS Label Stack**

The MPLS label stack size depends on the configuration of the core MPLS network:

- AToM uses one MPLS label to identify the AToM VCs (VC label). Therefore, the minimum MPLS label stack is one for directly connected AToM PEs, which are PE routers that do not have a P router between them.
- If LDP is used in the MPLS network, the label stack size is two (the LDP label and the VC label).
- If a TE tunnel instead of LDP is used between PE routers in the MPLS network, the label stack size is two (the TE label and the VC label).
- If a TE tunnel and LDP are used in the MPLS network (for example, a TE tunnel between P routers or between P and PE routers, with LDP on the tunnel), the label stack is three (TE label, LDP label, VC label).
- If you use MPLS fast reroute in the MPLS network, you add a label to the stack. The maximum MPLS label stack in this case is four (FRR label, TE label, LDP label, VC label).
- If AToM is used by the customer carrier in an MPLS VPN Carrier Supporting Carrier environment, you add a label to the stack. The maximum MPLS label stack in the provider carrier network is five (FRR label, TE label, LDP label, VPN label, VC label).
- If an AToM tunnel spans different service providers that exchange MPLS labels using IPv4 Border Gateway Protocol (BGP) (RFC 3107), you add a label to the stack. The maximum MPLS label stack is five (FRR label, TE label, Border Gateway Protocol (BGP) label, LDP label, VC label).

Other circumstances can increase the MPLS label stack size. Therefore, analyze the complete data path between the AToM tunnel endpoints and determine the maximum MPLS label stack size for your network. Then multiply the label stack size by the size of the MPLS label.

**Estimating Packet Size: Example**

The size of packets is estimate in the following example, which uses the following assumptions:

- The edge MTU is 1500 bytes.
- The transport type is Ethernet VLAN, which designates 18 bytes for the transport header.
- The AToM header is 0, because the control word is not used.
- The MPLS label stack is 2, because LDP is used. The MPLS label is 4 bytes.

$$\begin{array}{rcccccccc} \text{Edge MTU} & + & \text{Transport header} & + & \text{AToM header} & + & (\text{MPLS label stack} & * & \text{MPLS label}) & = & \text{Core MTU} \\ 1500 & & + 18 & & + 0 & & + (2 & & * 4 & & ) = 1526 \end{array}$$

You must configure the P and PE routers in the core to accept packets of 1526 bytes.

Once you determine the MTU size to set on your P and PE routers, you can issue the **mtu** command on the routers to set the MTU size. The following example specifies an MTU of 1526 bytes:

```
Router(config-if)# mtu 1526
```

## mpls mtu Command Changes

Some interfaces (such as FastEthernet) require the **mpls mtu** command to change the MTU size. In Cisco IOS Release 12.2(25)S, the behavior of the **mpls mtu** command changed.

If the interface MTU is fewer than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).



### Caution

Although you can set the MPLS MTU to a value greater than the interface MTU, set the MPLS MTU less than or equal to the interface MTU to prevent data corruption, dropped packets, and high CPU rates.

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and the interface MTU is 1500 bytes, the MPLS MTU range is 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S and you have an MPLS MTU setting that does not conform to these guidelines, the command is rejected.

For Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases, you cannot set the MPLS MTU greater than the interface MTU. This eliminates problems, such as dropped packets, data corruption, and high CPU rates. See the [MPLS MTU Command Changes](#) document for more information.

## Frame Relay over MPLS and DTE, DCE, and NNI Connections

You can configure an interface as a DTE device or a DCE switch, or as a switch connected to a switch with network-to-network interface (NNI) connections. Use the following command in interface configuration mode:

```
frame-relay intf-type [dce | dte | nni]
```

The keywords are explained in [Table 2](#).

**Table 2** *frame-relay intf-type Command Keywords*

| Keyword    | Description                                                                          |
|------------|--------------------------------------------------------------------------------------|
| <b>dce</b> | Enables the router or access server to function as a switch connected to a router.   |
| <b>dte</b> | Enables the router or access server to function as a DTE device. DTE is the default. |
| <b>nni</b> | Enables the router or access server to function as a switch connected to a switch.   |

## Local Management Interface and Frame Relay over MPLS

Local Management Interface (LMI) is a protocol that communicates status information about PVCs. When a PVC is added, deleted, or changed, the LMI notifies the endpoint of the status change. LMI also provides a polling mechanism that verifies that a link is up.

### How LMI Works

To determine the PVC status, LMI checks that a PVC is available from the reporting device to the Frame Relay end-user device. If a PVC is available, LMI reports that the status is “Active,” which means that all interfaces, line protocols, and core segments are operational between the reporting device and the Frame Relay end-user device. If any of those components is not available, the LMI reports a status of “Inactive.”

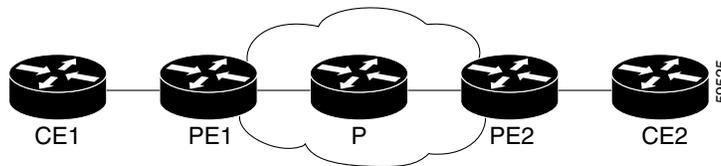


#### Note

Only the DCE and NNI interface types can report LMI status.

Figure 1 is a sample topology that helps illustrate how LMI works.

**Figure 1** Sample Topology



In Figure 1, note the following:

- CE1 and PE1 and PE2 and CE2 are Frame Relay LMI peers.
- CE1 and CE2 can be Frame Relay switches or end-user devices.
- Each Frame Relay PVC comprises multiple segments.
- The DLCI value is local to each segment and is changed as traffic is switched from segment to segment. Two Frame Relay PVC segments exist in Figure 1; one is between PE1 and CE1 and the other is between PE2 and CE2.

The LMI protocol behavior depends on whether you have DLCI-to-DLCI or port-to-port connections.

#### DLCI-to-DLCI Connections

If you have DLCI-to-DLCI connections, LMI runs locally on the Frame Relay ports between the PE and CE devices:

- CE1 sends an active status to PE1 if the PVC for CE1 is available. If CE1 is a switch, LMI checks that the PVC is available from CE1 to the user device attached to CE1.
- PE1 sends an active status to CE1 if the following conditions are met:
  - A PVC for PE1 is available.
  - PE1 received an MPLS label from the remote PE router.
  - An MPLS tunnel label exists between PE1 and the remote PE.

For DTE or DCE configurations, the following LMI behavior exists: The Frame Relay device accessing the network (DTE) does not report PVC status. Only the network device (DCE) or NNI can report status. Therefore, if a problem exists on the DTE side, the DCE is not aware of the problem.

#### Port-to-Port Connections

If you have port-to-port connections, the PE routers do not participate in the LMI status-checking procedures. LMI operates between the CE routers only. The CE routers must be configured as DCE-DTE or NNI-NNI.

For information about LMI, including configuration instructions, see the “Configuring the LMI” section of the *Configuring Frame Relay* document.

## QoS Features Supported with AToM

For information about configuring QoS features on the Cisco 12000 series routers, see the following feature module:

*Any Transport over MPLS (AToM): Layer 2 QoS for the Cisco 12000 Series Router (Quality of Service)*

The following tables list the QoS features supported by AToM on the Cisco 7200 and 7500 series routers:

- [Table 3, QoS Features Supported with Ethernet over MPLS on the Cisco 7200 and 7500 Series Routers](#)
- [Table 4, QoS Features Supported with Frame Relay over MPLS on the Cisco 7200 and 7500 Series Routers](#)
- [Table 5, QoS Features Supported with ATM Cell Relay and AAL5 over MPLS on the Cisco 7200 and 7500 Series Routers](#)

**Table 3** *QoS Features Supported with Ethernet over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature    | Ethernet over MPLS                                                                                                                                                                                                                                                                                             |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service policy | Can be applied to: <ul style="list-style-type: none"> <li>• Interface (input and output)</li> <li>• Subinterface (input and output)</li> </ul>                                                                                                                                                                 |
| Classification | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>match cos</b> (on interfaces and subinterfaces)</li> <li>• <b>match mpls experimental</b> (on interfaces and subinterfaces)</li> <li>• <b>match qos-group</b> (on interfaces) (output policy)</li> </ul>                          |
| Marking        | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>set cos</b> (output policy)</li> <li>• <b>set discard-class</b> (input policy)</li> <li>• <b>set mpls experimental</b> (input policy) (on interfaces and subinterfaces)</li> <li>• <b>set qos-group</b> (input policy)</li> </ul> |

**Table 3** *QoS Features Supported with Ethernet over MPLS on the Cisco 7200 and 7500 Series Routers (continued)*

| QoS Feature          | Ethernet over MPLS                                                                                                                                                                                            |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policing             | Supports the following: <ul style="list-style-type: none"> <li>• Single-rate policing</li> <li>• Two-rate policing</li> <li>• Color-aware policing</li> <li>• Multiple-action policing</li> </ul>             |
| Queueing and shaping | Supports the following: <ul style="list-style-type: none"> <li>• Distributed Low Latency Queueing (dLLQ)</li> <li>• Distributed Weighted Random Early Detection (dWRED)</li> <li>• Byte-based WRED</li> </ul> |

**Table 4** *QoS Features Supported with Frame Relay over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature    | Frame Relay over MPLS                                                                                                                                                                                                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service policy | Can be applied to: <ul style="list-style-type: none"> <li>• Interface (input and output)</li> <li>• PVC (input and output)</li> </ul>                                                                                                                                                                                                                                               |
| Classification | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>match fr-de</b> (on interfaces and VCs)</li> <li>• <b>match fr-dlci</b> (on interfaces)</li> <li>• <b>match qos-group</b></li> </ul>                                                                                                                                                                   |
| Marking        | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>frame-relay congestion management</b> (output)</li> <li>• <b>set discard-class</b></li> <li>• <b>set fr-de</b> (output policy)</li> <li>• <b>set fr-fecn-becn</b> (output)</li> <li>• <b>set mpls experimental</b></li> <li>• <b>set qos-group</b></li> <li>• <b>threshold ecn</b> (output)</li> </ul> |

**Table 4** *QoS Features Supported with Frame Relay over MPLS on the Cisco 7200 and 7500 Series Routers (continued)*

| QoS Feature          | Frame Relay over MPLS                                                                                                                                                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policing             | Supports the following: <ul style="list-style-type: none"> <li>• Single-rate policing</li> <li>• Two-rate policing</li> <li>• Color-aware policing</li> <li>• Multiple-action policing</li> </ul>                                                                                                  |
| Queueing and shaping | Supports the following: <ul style="list-style-type: none"> <li>• dLLQ</li> <li>• dWRED</li> <li>• Distributed traffic shaping</li> <li>• Distributed class-based weighted fair queueing (dCBWFQ)</li> <li>• Byte-based WRED</li> <li>• <b>random-detect discard-class-based</b> command</li> </ul> |

**Table 5** *QoS Features Supported with ATM Cell Relay and AAL5 over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature    | ATM Cell Relay and AAL5 over MPLS                                                                                                                                                                                                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service policy | Can be applied to: <ul style="list-style-type: none"> <li>• Interface (input and output)</li> <li>• Subinterface (input and output)</li> <li>• PVC (input and output)</li> </ul>                                                                                                                                                                                                             |
| Classification | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>match mpls experimental</b> (on VCs)</li> <li>• <b>match qos-group</b> (output)</li> </ul>                                                                                                                                                                                                                      |
| Marking        | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>random-detect discard-class-based</b> (input)</li> <li>• <b>set clp</b> (output) (on interfaces, subinterfaces, and VCs)</li> <li>• <b>set discard-class</b> (input)</li> <li>• <b>set mpls experimental</b> (input) (on interfaces, subinterfaces, and VCs)</li> <li>• <b>set qos-group</b> (input)</li> </ul> |

**Table 5** *QoS Features Supported with ATM Cell Relay and AAL5 over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature          | ATM Cell Relay and AAL5 over MPLS                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policing             | Supports the following: <ul style="list-style-type: none"> <li>• Single-rate policing</li> <li>• Two-rate policing</li> <li>• Color-aware policing</li> <li>• Multiple-action policing</li> </ul>                                                      |
| Queueing and shaping | Supports the following: <ul style="list-style-type: none"> <li>• dLLQ</li> <li>• dWRED</li> <li>• dCBWFQ</li> <li>• Byte-based WRED</li> <li>• random-detect discard-class-based command</li> <li>• Class-based shaping support on ATM PVCs</li> </ul> |

## How to Configure Any Transport over MPLS

This section explains how to perform a basic AToM configuration and includes the following procedures:

- [Configuring the Pseudowire Class, page 15](#) (required)
- [Configuring ATM AAL5 over MPLS on PVCs, page 16](#) (optional)
- [Configuring ATM AAL5 over MPLS in VC Class Configuration Mode, page 18](#) (optional)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS, page 21](#) (optional)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS on PVCs, page 21](#) (optional)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS in VC Class Configuration Mode, page 24](#) (optional)
- [Configuring ATM Cell Relay over MPLS in VC Mode, page 27](#) (optional)
- [Configuring ATM Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode, page 29](#) (optional)
- [Configuring ATM Cell Relay over MPLS in PVP Mode, page 31](#) (optional)
- [Configuring ATM Cell Relay over MPLS in Port Mode, page 34](#) (optional)
- [Configuring ATM Single Cell Relay over MPLS, page 36](#) (optional)
- [Configuring ATM Packed Cell Relay over MPLS, page 37](#) (optional)
- [Configuring Ethernet over MPLS in VLAN Mode, page 50](#) (optional)
- [Configuring Ethernet over MPLS in Port Mode, page 51](#) (optional)
- [Configuring Ethernet over MPLS with VLAN ID Rewrite, page 53](#) (optional)
- [Configuring Per Subinterface MTU for Ethernet over MPLS, page 58](#) (optional)
- [Configuring Frame Relay over MPLS with DLCI-to-DLCI Connections, page 61](#) (optional)

- [Configuring Frame Relay over MPLS with Port-to-Port Connections, page 62](#) (optional)
- [Configuring HDLC and PPP over MPLS, page 63](#) (optional)
- [Configuring Tunnel Selection, page 64](#) (optional)
- [Setting Experimental Bits with AToM, page 70](#) (optional)
- [Setting the Frame Relay Discard Eligibility Bit on the Cisco 7200 and 7500 Series Routers, page 73](#) (optional)
- [Matching the Frame Relay DE Bit on the Cisco 7200 and 7500 Series Routers, page 75](#) (optional)

## Configuring the Pseudowire Class

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. You set up the connection, called a pseudowire, between the routers.



### Note

---

In simple configurations, this task is optional. You do not need to specify a pseudowire class if you specify the tunneling method as part of the **xconnect** command.

---

The pseudowire-class configuration group specifies the following characteristics of the tunneling mechanism:

- Encapsulation type
- Control protocol
- Payload-specific options

For more information about the **pseudowire-class** command, see the following feature module:

### *Layer 2 Tunnel Protocol Version 3*

You must specify the **encapsulation mpls** command as part of the pseudowire class or as part of the **xconnect** command for the AToM VCs to work properly. If you omit the **encapsulation mpls** command as part of the **xconnect** command, you receive the following error:

```
% Incomplete command.
```

Once you specify the **encapsulation mpls** command, you cannot remove it using the **no encapsulation mpls** command. Nor can you change the command's setting using the **encapsulation l2tpv3** command. Those methods result in the following error message:

```
Encapsulation changes are not allowed on an existing pw-class.
```

To remove the command, you must delete the pseudowire with the **no pseudowire-class** command. To change the type of encapsulation, remove the pseudowire with the **no pseudowire-class** command and reestablish the pseudowire and specify the new encapsulation type.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class name**
4. **encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                            | Purpose                                                                                                     |
|--------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                       | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal               | Enters global configuration mode.                                                                           |
| Step 3 | <b>pseudowire-class name</b><br><br><b>Example:</b><br>Router(config)# pseudowire-class atom | Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode. |
| Step 4 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw)# encapsulation mpls    | Specifies the tunneling encapsulation.                                                                      |

## Configuring ATM AAL5 over MPLS on PVCs

ATM AAL5 over MPLS for permanent virtual circuits encapsulates ATM AAL5 service data unit (SDUs) in MPLS packets and forwards them across the MPLS network. Each ATM AAL5 SDU is transported as a single packet.

## Restrictions

AAL5 over MPLS is supported only in SDU mode.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface typeslot/port**
4. **pvc [name] vpi/vci l2transport**
5. **encapsulation aal5**
6. **xconnect peer-router-id vcid encapsulation mpls**
7. **exit**
8. **exit**
9. **exit**
10. **show mpls l2transport vc**

## DETAILED STEPS

|         | Command or Action                                                                                                                                                             | Purpose                                                                                                                                                                                                                                    |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                          |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                | Enters global configuration mode.                                                                                                                                                                                                          |
| Step 3  | <b>interface</b> <i>typeslot/port</i><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                              | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                           |
| Step 4  | <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i> <b>l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                               | Creates or assigns a name to an ATM PVC and enters L2transport configuration mode.<br><ul style="list-style-type: none"><li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li></ul> |
| Step 5  | <b>encapsulation aal5</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aal5                                                                     | Specifies ATM AAL5 encapsulation for the PVC. Make sure you specify the same encapsulation type on the PE and customer edge (CE) routers.                                                                                                  |
| Step 6  | <b>xconnect</b> <i>peer-router-id vcid</i> <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                           |
| Step 7  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                                 | Exits L2transport configuration mode.                                                                                                                                                                                                      |
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                 | Exits interface configuration mode.                                                                                                                                                                                                        |
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                    | Exits global configuration mode.                                                                                                                                                                                                           |
| Step 10 | <b>show mpls l2transport vc</b><br><br><b>Example:</b><br>Router# show mpls l2transport vc                                                                                    | Displays output that shows ATM AAL5 over MPLS is configured on a PVC.                                                                                                                                                                      |

## Examples

The following example enables ATM AAL5 over MPLS on an ATM PVC:

```
enable
configure terminal
interface atm1/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
```

The following is example output from the **show mpls l2transport vc**, which shows that ATM AAL5 over MPLS is configured on a PVC:

```
Router# show mpls l2transport vc
```

| Local intf | Local circuit  | Dest address | VC ID | Status |
|------------|----------------|--------------|-------|--------|
| -----      | -----          | -----        | ----- | -----  |
| ATM1/0     | ATM AAL5 1/100 | 10.4.4.4     | 100   | UP     |

## Configuring ATM AAL5 over MPLS in VC Class Configuration Mode

You can create a VC class that specifies the AAL5 encapsulation and then attach the encapsulation type to an interface, subinterface, or PVC. The following task creates a VC class and attaches it to a main interface.

### Restriction

AAL5 over MPLS is supported only in SDU mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **encapsulation** *layer-type*
5. **exit**
6. **interface** *typeslot/port*
7. **class-int** *vc-class-name*
8. **pvc** [*name*] *vpi/vci* **l2transport**
9. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**
10. **exit**
11. **exit**
12. **exit**
13. **show atm class-links**

## DETAILED STEPS

|         | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                      |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                             |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                  | Enters global configuration mode.                                                                                                                                                                                                            |
| Step 3  | <b>vc-class atm vc-class-name</b><br><br><b>Example:</b><br>Router(config)# vc-class atm aal5class                                                              | Creates a VC class and enters VC class configuration mode.                                                                                                                                                                                   |
| Step 4  | <b>encapsulation layer-type</b><br><br><b>Example:</b><br>Router(config-vc-class)# encapsulation aal5                                                           | Configures the AAL and encapsulation type.                                                                                                                                                                                                   |
| Step 5  | <b>exit</b><br><br><b>Example:</b><br>Router(config-vc-class)# exit                                                                                             | Exits VC class configuration mode.                                                                                                                                                                                                           |
| Step 6  | <b>interface typeslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                       | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                             |
| Step 7  | <b>class-int vc-class-name</b><br><br><b>Example:</b><br>Router(config-if)# class-int aal5class                                                                 | Applies a VC class to the ATM main interface or subinterface.<br><b>Note</b> You can also apply a VC class to a PVC.                                                                                                                         |
| Step 8  | <b>pvc [name] vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                                        | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul> |
| Step 9  | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                             |
| Step 10 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                   | Exits L2transport configuration mode.                                                                                                                                                                                                        |

|         |                                                                                         |                                                                                       |
|---------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Step 11 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                      | Exits interface configuration mode.                                                   |
| Step 12 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config)# exit</p>                         | Exits global configuration mode.                                                      |
| Step 13 | <pre>show atm class-links</pre> <p><b>Example:</b><br/>Router# show atm class-links</p> | Displays the type of encapsulation and that the VC class was applied to an interface. |

## Examples

The following example configures ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
enable
configure terminal
vc-class atm aal5class
encapsulation aal5
interface atm1/0
class-int aal5class
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```
enable
configure terminal
vc-class atm aal5class
encapsulation aal5
interface atm1/0
pvc 1/200 l2transport
class-vc aal5class
xconnect 10.13.13.13 100 encapsulation mpls
```

In the following example, the command output of the **show atm class-links** command verifies that ATM AAL5 over MPLS is configured as part of a VC class. The command output shows the type of encapsulation and that the VC class was applied to an interface.

```
Router# show atm class-links 1/100
```

```
Displaying vc-class inheritance for ATM1/0.0, vc 1/100:
no broadcast - Not configured - using default
encapsulation aal5 - VC-class configured on main interface
```

## Configuring OAM Cell Emulation for ATM AAL5 over MPLS

If a PE router does not support the transport of Operation, Administration, and Maintenance (OAM) cells across a label switched path (LSP), you can use OAM cell emulation to locally terminate or loop back the OAM cells. You configure OAM cell emulation on both PE routers, which emulates a VC by forming two unidirectional LSPs. You use the **oam-ac emulation-enable** and **oam-pvc manage** commands on both PE routers to enable OAM cell emulation.

After you enable OAM cell emulation on a router, you can configure and manage the ATM VC in the same manner as you would a terminated VC. A VC that has been configured with OAM cell emulation can send loopback cells at configured intervals toward the local CE router. The endpoint can be either of the following:

- End-to-end loopback, which sends OAM cells to the local CE router.
- Segment loopback, which responds to OAM cells to a device along the path between the PE and CE routers.

The OAM cells include the following cells:

- Alarm indication signal (AIS)
- Remote defect indication (RDI)

These cells identify and report defects along a VC. When a physical link or interface failure occurs, intermediate nodes insert OAM AIS cells into all the downstream devices affected by the failure. When a router receives an AIS cell, it marks the ATM VC down and sends an RDI cell to let the remote end know about the failure.

This section contains two tasks:

- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS on PVCs, page 21](#)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS in VC Class Configuration Mode, page 24](#)

### Configuring OAM Cell Emulation for ATM AAL5 over MPLS on PVCs

Perform this task to configure OAM cell emulation for ATM AAL5 over MPLS on a PVC.

**Note**

For AAL5 over MPLS, you can configure the **oam-pvc manage** command only after you issue the **oam-ac emulation-enable** command.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *typeslot/port*
4. **pvc** [*name*] *vpi/vci* **l2transport**
5. **encapsulation aal5**
6. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**
7. **oam-ac emulation-enable** [*ais-rate*]
8. **oam-pvc manage** [*frequency*]

9. **exit**
10. **exit**
11. **exit**
12. **show atm pvc**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                               | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                  |
| Step 3 | <b>interface</b> <i>typeslot/port</i><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                                     | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                                                                   |
| Step 4 | <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i> <b>l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                                      | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode.<br><ul style="list-style-type: none"><li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li></ul>                                      |
| Step 5 | <b>encapsulation aal5</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aal5                                                                            | Specifies ATM AAL5 encapsulation for the PVC. Make sure you specify the same encapsulation type on the PE and CE routers.                                                                                                                                                          |
| Step 6 | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i> <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                   |
| Step 7 | <b>oam-ac emulation-enable</b> [ <i>ais-rate</i> ]<br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30                                           | Enables OAM cell emulation for AAL5 over MPLS. The <i>ais-rate</i> argument lets you specify the rate at which AIS cells are sent. The default is one cell every second. The range is 0 to 60 seconds.                                                                             |
| Step 8 | <b>oam-pvc manage</b> [ <i>frequency</i> ]<br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# oam-pvc manage                                                               | Enables the PVC to generate end-to-end OAM loopback cells that verify connectivity on the virtual circuit.<br><br>The optional <i>frequency</i> argument is the interval between transmission of loopback cells and ranges from 0 to 600 seconds. The default value is 10 seconds. |

|                |                                                                               |                                                                          |
|----------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Step 9</b>  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit | Exits L2transport configuration mode.                                    |
| <b>Step 10</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                 | Exits interface configuration mode.                                      |
| <b>Step 11</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                    | Exits global configuration mode.                                         |
| <b>Step 12</b> | <b>show atm pvc</b><br><br><b>Example:</b><br>Router# show atm pvc            | Displays output that shows OAM cell emulation is enabled on the ATM PVC. |

## Examples

The following example enables OAM cell emulation on an ATM PVC:

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
oam-ac emulation-enable
oam-pvc manage
```

The following example sets the rate at which an AIS cell is sent every 30 seconds:

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
oam-ac emulation-enable 30
oam-pvc manage
```

The output of the **show atm pvc** command in the following example shows that OAM cell emulation is enabled on the ATM PVC:

```
Router# show atm pvc 5/500

ATM4/1/0.200: VCD: 6, VPI: 5, VCI: 500
UBR, PeakRate: 1
AAL5-LLC/SNAP, etype:0x0, Flags: 0x34000C20, VCmode: 0x0
OAM Cell Emulation: enabled, F5 End2end AIS Xmit frequency: 1 second(s)
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not ManagedVerified
ILMI VC state: Not Managed
InPkts: 564, OutPkts: 560, InBytes: 19792, OutBytes: 19680
InPRoc: 0, OutPRoc: 0
InFast: 4, OutFast: 0, InAS: 560, OutAS: 560
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
Out CLP=1 Pkts: 0
```

```
OAM cells received: 26
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 26
OAM cells sent: 77
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutAIS: 77, F5 OutRDI: 0
OAM cell drops: 0
Status: UP
```

## Configuring OAM Cell Emulation for ATM AAL5 over MPLS in VC Class Configuration Mode

The following steps explain how to configure OAM cell emulation as part of a VC class. You can then apply the VC class to an interface, a subinterface, or a VC. When you configure OAM cell emulation in VC class configuration mode and then apply the VC class to an interface, the settings in the VC class apply to all the VCs on the interface, unless you specify a different OAM cell emulation value at a lower level, such as the subinterface or VC level. For example, you can create a VC class that specifies OAM cell emulation and sets the rate of AIS cells to every 30 seconds. You can apply the VC class to an interface. Then, for one PVC, you can enable OAM cell emulation and set the rate of AIS cells to every 15 seconds. All the PVCs on the interface use the cell rate of 30 seconds, except for the one PVC that was set to 15 seconds.

Perform this task to enable OAM cell emulation as part of a VC class and apply it to an interface.



### Note

For AAL5 over MPLS, you can configure the **oam-pvc manage** command only after you issue the **oam-ac emulation-enable** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **encapsulation** *layer-type*
5. **oam-ac emulation-enable** [*ais-rate*]
6. **oam-pvc manage** [*frequency*]
7. **exit**
8. **interface** *typeslot/port*
9. **class-int** *vc-class-name*
10. **pvc** [*name*] *vpi/vci l2transport*
11. **xconnect** *peer-router-id vcid encapsulation mpls*

## DETAILED STEPS

|        | Command or Action                                                                                                       | Purpose                                                                                                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                          | Enters global configuration mode.                                                                                                                                                                                                                                                  |
| Step 3 | <b>vc-class atm name</b><br><br><b>Example:</b><br>Router(config)# vc-class atm oamclass                                | Creates a VC class and enters VC class configuration mode.                                                                                                                                                                                                                         |
| Step 4 | <b>encapsulation layer-type</b><br><br><b>Example:</b><br>Router(config-vc-class)# encapsulation aal5                   | Configures the AAL and encapsulation type.                                                                                                                                                                                                                                         |
| Step 5 | <b>oam-ac emulation-enable [ais-rate]</b><br><br><b>Example:</b><br>Router(config-vc-class)# oam-ac emulation-enable 30 | Enables OAM cell emulation for AAL5 over MPLS. The <i>ais-rate</i> argument lets you specify the rate at which AIS cells are sent. The default is one cell every second. The range is 0 to 60 seconds.                                                                             |
| Step 6 | <b>oam-pvc manage [frequency]</b><br><br><b>Example:</b><br>Router(config-vc-class)# oam-pvc manage                     | Enables the PVC to generate end-to-end OAM loopback cells that verify connectivity on the virtual circuit.<br><br>The optional <i>frequency</i> argument is the interval between transmission of loopback cells and ranges from 0 to 600 seconds. The default value is 10 seconds. |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vc-class)# exit                                                     | Exits VC class configuration mode.                                                                                                                                                                                                                                                 |
| Step 8 | <b>interface typeslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                               | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                                                                   |
| Step 9 | <b>class-int vc-class-name</b><br><br><b>Example:</b><br>Router(config-if)# class-int oamclass                          | Applies a VC class to the ATM main interface or subinterface.<br><br><b>Note</b> You can also apply a VC class to a PVC.                                                                                                                                                           |

|                |                                                                                                                                                                      |                                                                                                                                                                                                                                                     |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 10</b> | <pre>pvc [name] vpi/vci l2transport</pre> <p><b>Example:</b><br/>Router(config-if)# pvc 1/200 l2transport</p>                                                        | <p>Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul> |
| <b>Step 11</b> | <pre>xconnect peer-router-id vcid encapsulation mpls</pre> <p><b>Example:</b><br/>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls</p> | <p>Binds the attachment circuit to a pseudowire VC.</p>                                                                                                                                                                                             |

## Examples

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
class-int oamclass
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
pvc 1/200 l2transport
class-vc oamclass
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface. One PVC is configured with OAM cell emulation at an AIS rate of 10. That PVC uses the AIS rate of 10 instead of 30.

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
class-int oamclass
pvc 1/200 l2transport
oam-ac emulation-enable 10
xconnect 10.13.13.13 100 encapsulation mpls
```

## Configuring ATM Cell Relay over MPLS in VC Mode

Perform this task to configure ATM cell relay on the permanent virtual circuits.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm***slot/port*
4. **pvc** *vpi/vci* **l2transport**
5. **encapsulation aal0**
6. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**
7. **exit**
8. **exit**
9. **exit**
10. **show atm vc**

## DETAILED STEPS

|         | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                  |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                  | Enters global configuration mode.                                                                                                                                                                                                                                                 |
| Step 3  | <b>interface atmslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                        | Specifies an ATM interface and enters interface configuration mode.                                                                                                                                                                                                               |
| Step 4  | <b>pvc vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 0/100 l2transport                                                               | Assigns a virtual path identifier (VPI) and virtual circuit identifier (VCI) and enters L2transport VC configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul> |
| Step 5  | <b>encapsulation aa10</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aa10                                                       | For ATM cell relay, specifies raw cell encapsulation for the interface. Make sure you specify the same encapsulation type on the PE and CE routers.                                                                                                                               |
| Step 6  | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                  |
| Step 7  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                   | Exits L2transport configuration mode.                                                                                                                                                                                                                                             |
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                   | Exits interface configuration mode.                                                                                                                                                                                                                                               |
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                      | Exits global configuration mode.                                                                                                                                                                                                                                                  |
| Step 10 | <b>show atm vc</b><br><br><b>Example:</b><br>Router# show atm vc                                                                                                | Verifies that OAM cell emulation is enabled on the ATM VC.                                                                                                                                                                                                                        |

## Example

The output of the following **show atm vc** command shows that the interface is configured for VC mode cell relay:

```
Router# show atm vc 7

ATM3/0: VCD: 7, VPI: 23, VCI: 100
UBR, PeakRate: 149760
AAL0-Cell Relay, etype:0x10, Flags: 0x10000C2D, VCmode: 0x0
OAM Cell Emulation: not configured
InBytes: 0, OutBytes: 0
Status: UP
```

## Configuring ATM Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode

You can create a VC class that specifies the ATM cell relay encapsulation and then attach the VC class to an interface, subinterface, or VC. The following task creates a VC class that specifies the ATM cell relay encapsulation and attaches it to a main interface.



### Note

You can configure VC class configuration mode only in VC mode. VC class configuration mode is not supported on VP or port mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **encapsulation** *layer-type*
5. **exit**
6. **interface** *typeslot/port*
7. **class-int** *vc-class-name*
8. **pvc** [*name*] *vpi/vci* **l2transport**
9. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                  | Enters global configuration mode.                                                                                                                                                                                                             |
| Step 3 | <b>vc-class atm name</b><br><br><b>Example:</b><br>Router(config)# vc-class atm cellrelay                                                                       | Creates a VC class and enters VC class configuration mode.                                                                                                                                                                                    |
| Step 4 | <b>encapsulation layer-type</b><br><br><b>Example:</b><br>Router(config-vc-class)# encapsulation aal0                                                           | Configures the AAL and encapsulation type.                                                                                                                                                                                                    |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vc-class)# exit                                                                                             | Exits VC class configuration mode.                                                                                                                                                                                                            |
| Step 6 | <b>interface typeslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                       | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                              |
| Step 7 | <b>class-int vc-class-name</b><br><br><b>Example:</b><br>Router(config-if)# class-int cellrelay                                                                 | Applies a VC class to the ATM main interface or subinterface.<br><b>Note</b> You can also apply a VC class to a PVC.                                                                                                                          |
| Step 8 | <b>pvc [name] vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                                        | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode.<br><ul style="list-style-type: none"><li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li></ul> |
| Step 9 | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                              |

## Examples

The following example configures ATM cell relay over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
enable
```

```
configure terminal
vc-class atm cellrelay
encapsulation aal0
interface atm1/0
class-int cellrelay
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures ATM cell relay over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```
enable
configure terminal
vc-class atm cellrelay
encapsulation aal0
interface atm1/0
pvc 1/200 l2transport
class-vc cellrelay
xconnect 10.13.13.13 100 encapsulation mpls
```

## Configuring ATM Cell Relay over MPLS in PVP Mode

VP mode allows cells coming into a predefined PVP on the ATM interface to be transported over the MPLS backbone to a predefined PVP on the egress ATM interface. You can use VP mode to send single cells or packed cells over the MPLS backbone.

To configure VP mode, you must specify the following:

- The VP for transporting cell relay cells.
- The IP address of the peer PE router and the VC ID.

When configuring ATM cell relay over MPLS in VP mode, use the following guidelines:

- You do not need to enter the **encapsulation aal0** command in VP mode.
- One ATM interface can accommodate multiple types of ATM connections. VP cell relay, VC cell relay, and ATM AAL5 over MPLS can coexist on one ATM interface. On the Cisco 12000 series router, this is true only on the engine 0 ATM line cards.
- If a VPI is configured for VP cell relay, you cannot configure a PVC using the same VPI.
- VP trunking (mapping multiple VPs to one emulated VC label) is not supported. Each VP is mapped to one emulated VC.
- Each VP is associated with one unique emulated VC ID. The AToM emulated VC type is ATM VP cell transport.
- The AToM control word is supported. However, if a peer PE does not support the control word, it is disabled. This negotiation is done by LDP label binding.
- VP mode (and VC mode) drop idle cells.

Perform this task to configure ATM cell relay in PVP mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atmslot/port**
4. **atm pvp vpi l2transport**

5. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**
6. **exit**
7. **exit**
8. **exit**
9. **show atm vp**

## DETAILED STEPS

|        | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                  | Enters global configuration mode.                                                                                                                                                                                                                                       |
| Step 3 | <b>interface atm<sup>slot</sup>/<sub>port</sub></b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                  | Defines the interface and enters interface configuration mode.                                                                                                                                                                                                          |
| Step 4 | <b>atm pvp vpi l2transport</b><br><br><b>Example:</b><br>Router(config-if)# <b>atm pvp 1 l2transport</b>                                                        | Specifies that the PVP is dedicated to transporting ATM cells and enters l2transport PVP configuration submode.<br><br>The <b>l2transport</b> keyword indicates that the PVP is for cell relay. This submode is for Layer 2 transport only; it is not for regular PVPs. |
| Step 5 | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvp)#<br>xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports.                                                                                                                                           |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                   | Exits L2transport configuration mode.                                                                                                                                                                                                                                   |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                   | Exits interface configuration mode.                                                                                                                                                                                                                                     |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                      | Exits global configuration mode.                                                                                                                                                                                                                                        |
| Step 9 | <b>show atm vp</b><br><br><b>Example:</b><br>Router# show atm vp                                                                                                | Displays output that shows OAM cell emulation is enabled on the ATM VP.                                                                                                                                                                                                 |

## Examples

The following example transports single ATM cells over a virtual path:

```
pseudowire-class vp-cell-relay
encapsulation mpls
int atm 5/0
atm pvp 1 l2transport
xconnect 10.0.0.1 123 pw-class vp-cell-relay
```

The following **show atm vp** command in the following example shows that the interface is configured for VP mode cell relay:

```
Router# show atm vp 1
```

```
ATM5/0 VPI: 1, Cell Relay, PeakRate: 149760, CesRate: 0, DataVCs: 1, CesVCs: 0, Status:
ACTIVE
```

| VCD | VCI | Type | InPkts | OutPkts | AAL/Encap | Status |
|-----|-----|------|--------|---------|-----------|--------|
| 6   | 3   | PVC  | 0      | 0       | F4 OAM    | ACTIVE |
| 7   | 4   | PVC  | 0      | 0       | F4 OAM    | ACTIVE |

```
TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0,
TotalBroadcasts: 0 TotalInPktDrops: 0, TotalOutPktDrops: 0
```

## Configuring ATM Cell Relay over MPLS in Port Mode

Port mode cell relay allows cells coming into an ATM interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress ATM interface.

To configure port mode, issue the **xconnect** command from an ATM main interface and specify the destination address and the VC ID. The syntax of the **xconnect** command is the same as for all other transport types. Each ATM port is associated with one unique pseudowire VC label.

When configuring ATM cell relay over MPLS in port mode, use the following guidelines:

- The pseudowire VC type is set to ATM transparent cell transport (AAL0).
- The AToM control word is supported. However, if the peer PE does not support a control word, the control word is disabled. This negotiation is done by LDP label binding.
- Port mode and VP and VC mode are mutually exclusive. If you enable an ATM main interface for cell relay, you cannot enter any PVP or PVC commands.
- If the pseudowire VC label is withdrawn due to an MPLS core network failure, the PE router sends a line AIS to the CE router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm slot/port**
4. **xconnect peer-router-id vcid encapsulation mpls**
5. **exit**
6. **exit**
7. **show atm route**
8. **show mpls l2transport vc**

## DETAILED STEPS

|        | Command or Action                                                                                                                            | Purpose                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                               | Enters global configuration mode.                                                                                 |
| Step 3 | <b>interface atmslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                     | Specifies an ATM interface and enters interface configuration mode.                                               |
| Step 4 | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to the interface.                                                                    |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                | Exits interface configuration mode.                                                                               |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                   | Exits global configuration mode.                                                                                  |
| Step 7 | <b>show atm route</b><br><br><b>Example:</b><br>Router# show atm route                                                                       | Displays output that shows ATM cell relay in port mode has been enabled.                                          |
| Step 8 | <b>show mpls l2transport vc</b><br><br><b>Example:</b><br>Router# show mpls l2transport vc                                                   | Displays the attachment circuit and the interface.                                                                |

## Examples

The following example shows interface ATM 5/0 set up to transport ATM cell relay packets:

```
pseudowire-class atm-cell-relay
encapsulation mpls
interface atm 5/0
xconnect 10.0.0.1 123 pw-class atm-cell-relay
```

The **show atm route** command in the following example displays port mode cell relay state. The following example shows that atm interface 1/0 is for cell relay, the VC ID is 123 and the tunnel is down.

```
Router# show atm route
```

| Input Intf | Output Intf | Output VC | Status |
|------------|-------------|-----------|--------|
| ATM1/0     | ATOM Tunnel | 123       | DOWN   |

The `show mpls l2transport vc` command in the following example also shows configuration information.

```
Router# show mpls l2transport vc
```

| Local intf | Local circuit   | Dest address | VC ID | Status |
|------------|-----------------|--------------|-------|--------|
| AT1/0      | ATM CELL ATM1/0 | 10.1.1.121   | 1121  | UP     |

## Troubleshooting Tips

The `debug atm l2transport` and `debug mpls l2transport vc` display troubleshooting information.

## Configuring ATM Single Cell Relay over MPLS

The single cell relay feature allows you to insert one ATM cell in each MPLS packet. You can use single cell relay in both VP and VC mode. The configuration steps show how to configure single cell relay in VC mode. For VP mode, see the [“Configuring ATM Cell Relay over MPLS in PVP Mode”](#) section on page 31.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface atm slot/port`
4. `pvc vpi/vci l2transport`
5. `encapsulation aal0`
6. `xconnect peer-router-id vcid encapsulation mpls`

## DETAILED STEPS

|        | Command or Action                                                                                                                                            | Purpose                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                               | Enters global configuration mode.                                                                                                                                               |
| Step 3 | <b>interface atmslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                     | Specifies an ATM interface and enters interface configuration mode.                                                                                                             |
| Step 4 | <b>pvc vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/100 l2transport                                                            | Assigns a VPI and VCI and enters L2transport VC configuration mode.<br><br>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC. |
| Step 5 | <b>encapsulation aal0</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aal0                                                    | Specifies raw cell encapsulation for the interface. Make sure you specify the same encapsulation type on the PE and CE routers.                                                 |
| Step 6 | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                |

## Configuring ATM Packed Cell Relay over MPLS

The packed cell relay feature allows you to insert multiple concatenated ATM cells in an MPLS packet. The packed cell relay feature is more efficient than single cell relay, because each ATM cell is 52 bytes, and each AToM packet is at least 64 bytes.

At a high level, packed cell relay configuration consists of the following steps:

- You specify the amount of time a PE router can wait for cells to be packed into an MPLS packet. You can set up three timers by default with different amounts of time attributed to each timer.
- You enable packed cell relay, specify how many cells should be packed into each MPLS packet, and choose which timer to use during the cell packing process.

### Restrictions

- The **cell-packing** command is available only if you use AAL0 encapsulation in VC mode. If the command is configured with ATM AAL5 encapsulation, the command is not valid.

- Only cells from the same VC, VP, or port can be packed into one MPLS packet. Cells from different connections cannot be concatenated into the same MPLS packet.
- When you change, enable, or disable the cell-packing attributes, the ATM VC, VP, or port and the MPLS emulated VC are reestablished.
- If a PE router does not support packed cell relay, the PE router sends only one cell per MPLS packet.
- The number of packed cells does not need to match between the PE routers. The two PE routers agree on the lower of the two values. For example, if PE1 is allowed to pack 10 cells per MPLS packet and PE2 is allowed to pack 20 cells per MPLS packet, the two PE routers would agree to send no more than 10 cells per packet.
- If the number of cells packed by the peer PE router exceeds the limit, the packXet is dropped.
- Issue the **atm mcpt-timers** command on an ATM interface before issuing the **cell-packing** command.

See the following sections for configuration information:

- [Configuring ATM Packed Cell Relay over MPLS in VC Mode, page 38](#)
- [Configuring ATM Packed Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode, page 40](#)
- [Configuring ATM Packed Cell Relay over MPLS in VP Mode, page 44](#)
- [Configuring ATM Packed Cell Relay over MPLS in Port Mode, page 46](#)

## Configuring ATM Packed Cell Relay over MPLS in VC Mode

Perform this task to configure the ATM packed cell relay over MPLS feature in VC mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm***slot/port*
4. **shutdown**
5. **atm mcpt-timers** [*timer1-timeout timer2-timeout timer3-timeout*]
6. **no shutdown**
7. **pvc** *vpi/vci* **l2transport**
8. **encapsulation aal0**
9. **xconnect** *peer-router-id vcid* **encapsulation mpls**
10. **cell-packing** [*cells*] [**mcpt-timer** *timer*]

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                 | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <p><b>interface atmslot/port</b></p> <p><b>Example:</b><br/>Router(config)# interface atm1/0</p>                                                       | <p>Defines the interface and enters interface configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 4 | <p><b>shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# shutdown</p>                                                                          | <p>Shuts down the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <p><b>atm mcpt-timers</b> [timer1-timeout timer2-timeout timer3-timeout]</p> <p><b>Example:</b><br/>Router(config-if)# atm mcpt-timers 100 200 250</p> | <p>Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet.</p> <p>You can set up to three timers. For each timer, you specify the maximum cell-packing timeout (MCPT). This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</p> <p>The respective default values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>OC-3: 30, 60, and 90 microseconds</li> <li>T3: 100, 200, and 300 microseconds</li> <li>E3: 130, 260, and 390 microseconds</li> </ul> <p>You can specify either the number of microseconds or use the default.</p> <p>The respective range of values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>OC-3: 10 to 4095 microseconds</li> <li>T3: 30 to 4095 microseconds</li> <li>E3: 40 to 4095 microseconds</li> </ul> |
| Step 6 | <p><b>no shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# no shutdown</p>                                                                    | <p>Enables the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|         | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>pvc vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/100 l2transport                                                               | Assigns a VPI and VCI and enters L2transport VC configuration mode.<br><br><ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul>                                                                                                                                                                                                        |
| Step 8  | <b>encapsulation aa10</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)#<br>encapsulation aa10                                                    | Specifies raw cell encapsulation for the interface. Make sure you specify the same encapsulation type on the PE routers.                                                                                                                                                                                                                                                                                                                 |
| Step 9  | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect<br>10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 10 | <b>cell-packing [cells] [mcpt-timer timer]</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# cell-packing<br>10 mcpt-timer 1                     | Enables cell packing and specifies the cell-packing parameters.<br><br>The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52.<br><br>The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.<br><br>See the <b>cell-packing</b> command page for more information. |

## Examples

The following example shows that ATM PVC 1/100 is an AToM cell relay PVC. There are three timers set up, with values of 1000 milliseconds, 800 milliseconds, and 500 milliseconds, respectively. The **cell-packing** command specifies that five ATM cells are to be packed into an MPLS packet. The **cell-packing** command also specifies that timer 1 is to be used.

```
int atm 1/0
shutdown
atm mcpt-timer 1000 800 500
no shutdown
pvc 1/100 l2transport
encapsulation aa10
xconnect 10.0.0.1 123 encapsulation mpls
cell-packing 5 mcpt-timer 1
```

## Configuring ATM Packed Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode

You can create a VC class that specifies the ATM cell relay encapsulation and the cell packing parameters and then attach the VC class to an interface, subinterface, or VC. The following task creates a VC class that specifies the ATM cell relay encapsulation and cell packing and attaches it to a main interface.

**Note**

You can configure VC class configuration mode only in VC mode. VC class configuration mode is not supported on VP or port mode.

When you configure cell packing in VC class configuration mode and then apply the VC class to an interface, the settings in the VC class apply to all the VCs on the interface, unless you specify a different cell packing value at a lower level, such as the subinterface or VC level. For example, you can create a VC class that specifies three cells to be packed. You can apply the VC class to an interface. Then, for one PVC, you can specify two cells to be packed. All the PVCs on the interface pack three cells, except for the one PVC that was set to set two cells.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **encapsulation** *layer-type*
5. **cell-packing** [*cells*] [**mcpt-timer** *timer*]
6. **exit**
7. **interface** *typeslot/port*
8. **shutdown**
9. **atm mcpt-timers** [*timer1-timeout timer2-timeout timer3-timeout*]
10. **no shutdown**
11. **class-int** *vc-class-name*
12. **pvc** [*name*] *vpilvci* **l2transport**
13. **xconnect** *peer-router-id vcid* **encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                            | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>vc-class atm name</b><br><br><b>Example:</b><br>Router(config)# vc-class atm cellpacking                                       | Creates a VC class and enters VC class configuration mode.                                                                                                                                                                                                                                                                                                                                                                               |
| Step 4 | <b>encapsulation layer-type</b><br><br><b>Example:</b><br>Router(config-vc-class)# encapsulation aal0                             | Configures the AAL and encapsulation type.                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 5 | <b>cell-packing [cells] [mcpt-timer timer]</b><br><br><b>Example:</b><br>Router(config-vc-class)# cell-packing 10<br>mcpt-timer 1 | Enables cell packing and specifies the cell-packing parameters.<br><br>The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52.<br><br>The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.<br><br>See the <b>cell-packing</b> command page for more information. |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vc-class)# exit                                                               | Exits VC class configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7 | <b>interface typeslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                         | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                         |
| Step 8 | <b>shutdown</b><br><br><b>Example:</b><br>Router(config-if)# shutdown                                                             | Shuts down the interface.                                                                                                                                                                                                                                                                                                                                                                                                                |

|                |                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 9</b>  | <pre>atm mcpt-timers [timer1-timeout timer2-timeout timer3-timeout]</pre> <p><b>Example:</b><br/>Router(config-if)# atm mcpt-timers 100 200 250</p>                  | <p>Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet.</p> <p>You can set up to three timers. For each timer, you specify the MCPT. This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</p> <p>The respective default values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>• OC-3: 30, 60, and 90 microseconds</li> <li>• T3: 100, 200, and 300 microseconds</li> <li>• E3: 130, 260, and 390 microseconds</li> </ul> <p>You can specify either the number of microseconds or use the default.</p> <p>The respective range of values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>• OC-3: 10 to 4095 microseconds</li> <li>• T3: 30 to 4095 microseconds</li> <li>• E3: 40 to 4095 microseconds</li> </ul> |
| <b>Step 10</b> | <pre>no shutdown</pre> <p><b>Example:</b><br/>Router(config-if)# no shutdown</p>                                                                                     | <p>Enables the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 11</b> | <pre>class-int vc-class-name</pre> <p><b>Example:</b><br/>Router(config-if)# class-int cellpacking</p>                                                               | <p>Applies a VC class to the ATM main interface or subinterface.</p> <p><b>Note</b> You can also apply a VC class to a PVC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 12</b> | <pre>pvc [name] vpi/vci l2transport</pre> <p><b>Example:</b><br/>Router(config-if)# pvc 1/200 l2transport</p>                                                        | <p>Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode.</p> <ul style="list-style-type: none"> <li>• The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 13</b> | <pre>xconnect peer-router-id vcid encapsulation mpls</pre> <p><b>Example:</b><br/>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls</p> | <p>Binds the attachment circuit to a pseudowire VC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Examples

The following example configures ATM cell relay over MPLS with cell packing in VC class configuration mode. The VC class is then applied to an interface.

```
enable
```

```

configure terminal
vc-class atm cellpacking
encapsulation aal0
cell-packing 10 mcpt-timer 1
interface atm1/0
shutdown
atm mcpt-timers 100 200 250
no shutdown
class-int cellpacking
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls

```

The following example configures ATM cell relay over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```

enable
configure terminal
vc-class atm cellpacking
encapsulation aal0
cell-packing 10 mcpt-timer 1
interface atm1/0
shutdown
atm mcpt-timers 100 200 250
no shutdown
pvc 1/200 l2transport
class-vc cellpacking
xconnect 10.13.13.13 100 encapsulation mpls

```

## Configuring ATM Packed Cell Relay over MPLS in VP Mode

Perform this task to configure the ATM cell-packing feature in VP mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *atmslot/port***
4. **shutdown**
5. **atm mcpt-timers** [*timer1-timeout timer2-timeout timer3-timeout*]
6. **no shutdown**
7. **atm pvp *vpi* l2transport**
8. **xconnect *peer-router-id vcid* encapsulation mpls**
9. **cell-packing** [*cells*] [**mcpt-timer** *timer*]

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                 | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <p><b>interface atmslot/port</b></p> <p><b>Example:</b><br/>Router(config)# interface atm1/0</p>                                                       | <p>Defines the interface and enters interface configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <p><b>shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# shutdown</p>                                                                          | <p>Shuts down the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 5 | <p><b>atm mcpt-timers</b> [timer1-timeout timer2-timeout timer3-timeout]</p> <p><b>Example:</b><br/>Router(config-if)# atm mcpt-timers 100 200 250</p> | <p>Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet.</p> <p>You can set up to three timers. For each timer, you specify the MCPT. This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</p> <p>The respective default values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>OC-3: 30, 60, and 90 microseconds</li> <li>T3: 100, 200, and 300 microseconds</li> <li>E3: 130, 260, and 390 microseconds</li> </ul> <p>You can specify either the number of microseconds or use the default.</p> <p>The respective range of values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>OC-3: 10 to 4095 microseconds</li> <li>T3: 30 to 4095 microseconds</li> <li>E3: 40 to 4095 microseconds</li> </ul> |
| Step 6 | <p><b>no shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# no shutdown</p>                                                                    | <p>Enables the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|        | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>atm pvp vpi 12transport</b><br><br><b>Example:</b><br>Router(config-if)# <b>atm pvp 1 12transport</b>                                                  | Specifies that the PVP is dedicated to transporting ATM cells and enters L2transport PVP configuration submode.<br><br>The <b>12transport</b> keyword indicates that the PVP is for cell relay. This submode is for Layer 2 transport only; it is not for regular PVPs.                                                                                                                                                                  |
| Step 8 | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(cfg-if-atm-l2trans-pvp)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports.                                                                                                                                                                                                                                                                                                            |
| Step 9 | <b>cell-packing [cells] [mcpt-timer timer]</b><br><br><b>Example:</b><br>Router(cfg-if-atm-l2trans-pvp)# cell-packing 10 mcpt-timer 1                     | Enables cell packing and specifies the cell-packing parameters.<br><br>The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52.<br><br>The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.<br><br>See the <b>cell-packing</b> command page for more information. |

## Examples

The following example shows packed cell relay enabled on an interface set up for PVP mode. The **cell-packing** command specifies that 10 ATM cells are to be packed into an MPLS packet. The **cell-packing** command also specifies that timer 2 is to be used.

```
interface atm 1/0
shutdown
atm mcpt-timer 1000 800 500
no shutdown
atm pvp 100 12transport
xconnect 10.0.0.1 234 encapsulation mpls
cell-packing 10 mcpt-timer 2
```

## Configuring ATM Packed Cell Relay over MPLS in Port Mode

Perform this task to configure ATM packed cell relay over MPLS in port mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm slot/port**
4. **shutdown**
5. **atm mcpt-timers [timer1-timeout timer2-timeout timer3-timeout]**
6. **no shutdown**
7. **cell-packing [cells] [mcpt-timer timer]**
8. **xconnect peer-router-id vcid encapsulation mpls**

9. **exit**
10. **exit**
11. **show atm cell-packing**
12. **show atm vp**

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                 | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <p><b>interface atmslot/port</b></p> <p><b>Example:</b><br/>Router(config)# interface atml/0</p>                                                       | <p>Specifies an ATM interface and enters interface configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 4 | <p><b>shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# shutdown</p>                                                                          | <p>Shuts down the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 5 | <p><b>atm mcpt-timers</b> [timer1-timeout timer2-timeout timer3-timeout]</p> <p><b>Example:</b><br/>Router(config-if)# atm mcpt-timers 100 200 250</p> | <p>Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet.</p> <p>You can set up to three timers. For each timer, you specify the MCPT. This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</p> <p>The respective default values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>OC-3: 30, 60, and 90 microseconds</li> <li>T3: 100, 200, and 300 microseconds</li> <li>E3: 130, 260, and 390 microseconds</li> </ul> <p>You can specify either the number of microseconds or use the default.</p> <p>The respective range of values for the PA-A3 port adapters are:</p> <ul style="list-style-type: none"> <li>OC-3: 10 to 4095 microseconds</li> <li>T3: 30 to 4095 microseconds</li> <li>E3: 40 to 4095 microseconds</li> </ul> |
| Step 6 | <p><b>no shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# no shutdown</p>                                                                    | <p>Enables the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                |                                                                                    |                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 7</b>  | <b>cell-packing</b> [ <i>cells</i> ] [ <b>mcpt-timer</b> <i>timer</i> ]            | Enables cell packing and specifies the cell-packing parameters.                                                                                                                          |
|                | <b>Example:</b><br>Router(config-if)# cell-packing 10 mcpt-timer 1                 | The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52. |
|                |                                                                                    | The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.                                                                                              |
|                |                                                                                    | See the <b>cell-packing</b> command page for more information.                                                                                                                           |
| <b>Step 8</b>  | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i> <b>encapsulation</b> <b>mpls</b> | Binds the attachment circuit to the interface.                                                                                                                                           |
|                | <b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123 encapsulation mpls     |                                                                                                                                                                                          |
| <b>Step 9</b>  | <b>exit</b>                                                                        | Exits interface configuration mode.                                                                                                                                                      |
|                | <b>Example:</b><br>Router(config-if)# exit                                         |                                                                                                                                                                                          |
| <b>Step 10</b> | <b>exit</b>                                                                        | Exits global configuration mode.                                                                                                                                                         |
|                | <b>Example:</b><br>Router(config)# exit                                            |                                                                                                                                                                                          |
| <b>Step 11</b> | <b>show atm cell-packing</b>                                                       | Displays cell-packing statistics.                                                                                                                                                        |
|                | <b>Example:</b><br>Router# show atm cell-packing                                   |                                                                                                                                                                                          |
| <b>Step 12</b> | <b>show atm vp</b>                                                                 | Displays cell-packing information.                                                                                                                                                       |
|                | <b>Example:</b><br>Router#show atm vp                                              |                                                                                                                                                                                          |

## Examples

The following example shows packed cell relay enabled on an interface set up for port mode. The **cell-packing** command specifies that 10 ATM cells are to be packed into an MPLS packet. The **cell-packing** command also specifies that timer 2 is to be used.

```
interface atm 5/0
shutdown
atm mcpt-timer 1000 800 500
no shutdown
cell-packing 10 mcpt-timer 2
xconnect 10.0.0.1 123 encapsulation mpls
```

The **show atm cell-packing** command in the following example displays the following statistics:

- The number of cells that are to be packed into an MPLS packet on the local and peer routers
- The average number of cells sent and received

- The timer values associated with the local router

```
Router# show atm cell-packing
```

```

 circuit local average peer average
 type MNCP nbr of cells MNCP nbr of cells MCPT
 =====
atm 1/0 vc 1/200 20 15 30 20 60
atm 1/0 vp 2 25 21 30 24 100

```

The **show atm vp** command in the following example displays the cell packing information at the end of the output:

```
Router# show atm vp 12
```

```
ATM5/0 VPI: 12, Cell Relay, PeakRate: 149760, CesRate: 0, DataVCs: 1, CesVCs: 0, Status:
ACTIVE
```

```

VCD VCI Type InPkts OutPkts AAL/Encap Status
 6 3 PVC 0 0 F4 OAM ACTIVE
 7 4 PVC 0 0 F4 OAM ACTIVE

```

```

TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0,
TotalBroadcasts: 0 TotalInPktDrops: 0, TotalOutPktDrops: 0
Local MNCP: 5, average number of cells received: 3
Peer MNCP: 1, average number of cells sent: 1
Local MCPT: 100 us

```

## Troubleshooting Tips

To debug ATM cell packing, issue the **debug atm cell-packing** command.

## Configuring Ethernet over MPLS in VLAN Mode

A VLAN is a switched network that is logically segmented by functions, project teams, or applications regardless of the physical location of users. Ethernet over MPLS allows you to connect two VLAN networks that are in different locations. You configure the PE routers at each end of the MPLS backbone and add a point-to-point VC. Only the two PE routers at the ingress and egress points of the MPLS backbone know about the VCs dedicated to transporting Layer 2 VLAN traffic. All other routers do not have table entries for those VCs. Ethernet over MPLS in VLAN mode transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN over a core MPLS network.



### Note

You must configure Ethernet over MPLS (VLAN mode) on the subinterfaces.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet<slot>/interface.subinterface**
4. **encapsulation dot1q <vlan-id>**
5. **xconnect <peer-router-id> <vcid> encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                                                                                                                                   |
| Step 3 | <b>interface</b><br><b>gigabitethernet</b> <i>slot/interface.subinterface</i><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0.1 | Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode. Make sure the subinterface on the adjoining CE router is on the same VLAN as this PE router.                                                |
| Step 4 | <b>encapsulation dot1q</b> <i>vlan-id</i><br><br><b>Example:</b><br>Router(config-subif)# encapsulation dot1q 100                                      | Enables the subinterface to accept 802.1Q VLAN packets.<br><br>The subinterfaces between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet. All other subinterfaces and backbone routers do not. |
| Step 5 | <b>xconnect</b> <i>peer-router-id vcid encapsulation mpls</i><br><br><b>Example:</b><br>Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports.                                                                                                       |

## Configuring Ethernet over MPLS in Port Mode

Port mode allows a frame coming into an interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress interface. The entire Ethernet frame without the preamble or FCS is transported as a single packet. To configure port mode, you use the **xconnect** command in interface configuration mode and specify the destination address and the VC ID. The syntax of the **xconnect** command is the same as for all other transport types. Each interface is associated with one unique pseudowire VC label.

When configuring Ethernet over MPLS in port mode, use the following guidelines:

- The pseudowire VC type is set to Ethernet.
- Port mode and Ethernet VLAN mode are mutually exclusive. If you enable a main interface for port-to-port transport, you cannot also enter commands on a subinterface.

## SUMMARY STEPS

- enable**
- configure terminal**
- interface** **gigabitethernet***slot/interface*

4. `xconnect peer-router-id vcid encapsulation mpls`
5. `exit`
6. `exit`
7. `show mpls l2transport vc`

## DETAILED STEPS

|        | Command or Action                                                                                                                                  | Purpose                                                                                                                                                                     |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                          |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal                                                               | Enters global configuration mode.                                                                                                                                           |
| Step 3 | <code>interface gigabitethernet slot/interface</code><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0                       | Specifies the Gigabit Ethernet interface and enters interface configuration mode. Make sure the interface on the adjoining CE router is on the same VLAN as this PE router. |
| Step 4 | <code>xconnect peer-router-id vcid encapsulation mpls</code><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports.                                               |
| Step 5 | <code>exit</code><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                | Exits interface configuration mode.                                                                                                                                         |
| Step 6 | <code>exit</code><br><br><b>Example:</b><br>Router(config)# exit                                                                                   | Exits router configuration mode.                                                                                                                                            |
| Step 7 | <code>show mpls l2transport vc</code><br><br><b>Example:</b><br>Router# show mpls l2transport vc                                                   | Displays information about Ethernet over MPLS port mode.                                                                                                                    |

## Examples

The following example configures VC 123 in Ethernet port mode:

```
pseudowire-class ethernet-port
encapsulation mpls

int gigabitethernet1/0
```

```
xconnect 10.0.0.1 123 pw-class ethernet-port
```

The command output in the following example shows two VCs for Ethernet over MPLS:

- VC 2 is in Ethernet VLAN mode.
- VC 8 is in Ethernet port mode.

```
Router# show mpls l2transport vc
```

| Local intf | Local circuit | Dest address | VC ID | Status |
|------------|---------------|--------------|-------|--------|
| Gi4/0.1    | Eth VLAN 2    | 10.1.1.1     | 2     | UP     |
| Gi8/0/1    | Ethernet      | 10.1.1.1     | 8     | UP     |

If you issue the **show mpls l2transport vc detail** command, the output is similar:

```
Router# show mpls l2transport vc detail
```

```
Local interface: Gi4/0.1 up, line protocol up, Eth VLAN 2 up
Destination address: 10.1.1.1, VC ID: 2, VC status: up
.
.
.
Local interface: Gi8/0/1 up, line protocol up, Ethernet up
Destination address: 10.1.1.1, VC ID: 8, VC status: up
```

## Configuring Ethernet over MPLS with VLAN ID Rewrite

The VLAN ID rewrite feature enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.

The Cisco 12000 series router requires you to configure VLAN ID rewrite manually, as described in the following sections.

The following routers automatically perform VLAN ID rewrite on the disposition PE router. No configuration is required:

- Cisco 7200 series routers.
- Cisco 7500 series routers.
- Cisco 10720 series routers.
- Routers supported on Cisco IOS Release 12.4(11)T. (Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support.)

The following sections explain how to configure the VLAN ID rewrite feature:

- [Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0\(29\)S and Earlier Releases, page 53](#)
- [Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0\(30\)S and Later Releases, page 54](#)

## Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0(29)S and Earlier Releases

Use the following guidelines for the VLAN ID rewrite feature for the Cisco 12000 series routers in Cisco IOS releases earlier than 12.0(29)S:

- The IP Service Engine (ISE) 4-port Gigabit Ethernet line card performs the VLAN ID rewrite on the disposition side at the edge-facing line card.
- The engine 2 3-port Gigabit Ethernet line card performs the VLAN ID rewrite on the imposition side at the edge-facing line card.

The VLAN ID rewrite functionality requires that both ends of the Ethernet over MPLS connections be provisioned with the same line cards. Make sure that both edge-facing ends of the virtual circuit use either the engine 2 or ISE Ethernet line card. The following example shows the system flow with the VLAN ID rewrite feature:

- The ISE 4-port Gigabit Ethernet line card:  
Traffic flows from VLAN1 on CE1 to VLAN2 on CE2. As the frame reaches the edge-facing line card of the disposition router PE2, the VLAN ID in the dot1Q header changes to the VLAN ID assigned to VLAN2.
- The engine 2 3-port Gigabit Ethernet line card:  
Traffic flows from VLAN1 on CE1 to VLAN2 on CE2. As the frame reaches the edge-facing line card of the imposition router PE1, the VLAN ID in the dot1Q header changes to the VLAN ID assigned to VLAN2.

For the Cisco 12000 series router engine 2 3-port Gigabit Ethernet line card, you must issue the **remote circuit id** command as part of the Ethernet over MPLS VLAN ID rewrite configuration.

## Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0(30)S and Later Releases

In Cisco IOS Release 12.0(30)S, the following changes to VLAN ID rewrite were implemented:

- The ISE 4-port Gigabit Ethernet line card can perform VLAN ID rewrite at both the imposition and disposition sides of the edge-facing router.
- The **remote circuit id** command is not required as part of the Ethernet over MPLS VLAN ID rewrite configuration, as long as both PE routers are running Cisco IOS Release 12.0(30)S. The VLAN ID rewrite feature is implemented automatically when you configure Ethernet over MPLS.
- The VLAN ID rewrite feature in Cisco IOS Release 12.0(30)S can interoperate with routers that are running earlier releases. If you have a PE router at one end of the circuit that is using an earlier Cisco IOS release and the **remote circuit id** command, the other PE can run Cisco IOS Release 12.0(30)S and still perform VLAN ID rewrite.
- You can mix the line cards on the PE routers, as shown in the following table

**Table 6** Supported Line Cards for VLAN ID Rewrite Feature:

| If PE1 Has These Line Cards                                                               | Then PE2 Can Use These Line Cards                                                         |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Engine 2 3-port Gigabit Ethernet line card<br>or<br>ISE 4-port Gigabit Ethernet line card | Engine 2 3-port Gigabit Ethernet line card<br>or<br>ISE 4-port Gigabit Ethernet line card |
| ISE 4-port Gigabit Ethernet line card                                                     | Any Cisco 12000 series router line card                                                   |

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** `gigabitethernet`*slot/port.subinterface*
4. **encapsulation** `dot1q` *vlan-id*
5. **xconnect** *peer-router-id vcid* **encapsulation** `mpls`
6. **remote circuit id** *remote-vlan-id*
7. **exit**
8. **exit**
9. **exit**
10. **show controllers** `compls forwarding-table`

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface</b><br><b>gigabitethernet</b> <i>slot/interface.subinterface</i><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0.1 | Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode.<br><br>Make sure the subinterfaces between the CE and PE routers that are running Ethernet over MPLS are in the same subnet. All other subinterfaces and backbone routers do not need to be in the same subnet. |
| Step 4 | <b>encapsulation dot1q</b> <i>vlan-id</i><br><br><b>Example:</b><br>Router(config-subif)# encapsulation dot1q 100                                      | Enables the subinterface to accept 802.1Q VLAN packets.<br><br>Make sure the subinterface on the adjoining CE router is on the same VLAN as this PE router.                                                                                                                                             |
| Step 5 | <b>xconnect</b> <i>peer-router-id vcid encapsulation mpls</i><br><br><b>Example:</b><br>Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC and enters xconnect configuration mode. The syntax for this command is the same as for all other Layer 2 transports.                                                                                                                                    |
| Step 6 | <b>remote circuit id</b> <i>remote-vlan-id</i><br><br><b>Example:</b><br>Router(config-subif-xconn)# remote circuit id 101                             | Enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel. This command is required only for the Cisco 12000 series router engine 2 3-port Gigabit Ethernet line card.                                                                                                      |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-subif-xconn)# exit                                                                                 | Exits xconnect configuration mode.                                                                                                                                                                                                                                                                      |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-subif)# exit                                                                                       | Exits subinterface configuration mode.                                                                                                                                                                                                                                                                  |

|                |                                                                                                                                           |                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| <b>Step 9</b>  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                | Exits global configuration mode.            |
| <b>Step 10</b> | <b>show controllers eompls forwarding-table</b><br><br><b>Example:</b><br>Router# execute slot 0 show controllers eompls forwarding-table | Displays information about VLAN ID rewrite. |

## Examples

The following example configures VLAN ID rewrite on peer PE routers with Cisco 12000 series router engine 2 3-port Gigabit Ethernet line cards.

| PE1                                                                                                                                                               | PE2                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>interface GigabitEthernet0/0.2 encapsulation dot1Q 2 no ip directed-broadcast no cdp enable xconnect 10.5.5.5 2 encapsulation mpls remote circuit id 3</pre> | <pre>interface GigabitEthernet3/0.2 encapsulation dot1Q 3 no ip directed-broadcast no cdp enable xconnect 10.3.3.3 2 encapsulation mpls remote circuit id 2</pre> |

The command output of the **show controllers eompls forwarding-table** command in the following example shows VLAN ID rewrite configured on the Cisco 12000 series routers with an engine 2 3-port Gigabit Ethernet line card. In the following example, the bolded command output show the VLAN ID rewrite information.

### On PE1

```
Router# execute slot 0 show controllers eompls forwarding-table 0 2

Port # 0, VLAN-ID # 2, Table-index 2
EoMPLS configured: 1
tag_rew_ptr = D001BB58
Leaf entry? = 1
FCR index = 20
 **tagrew_psa_addr = 0006ED60
 **tagrew_vir_addr = 7006ED60
 **tagrew_phy_addr = F006ED60
[0-7] loq 8800 mtu 4458 oq 4000 ai 3 oi 04019110 (encaps size 4)
cw-size 4 vlanid-rew 3
gather A30 (bufhdr size 32 EoMPLS (Control Word) Imposition profile 81)
2 tag: 18 18
counters 1182, 10 reported 1182, 10.
Local OutputQ (Unicast): Slot:2 Port:0 RED queue:0 COS queue:0
Output Q (Unicast): Port:0 RED queue:0 COS queue:0
```

### On PE2

```
Router# execute slot 0 show controllers eompls forwarding-table 0 3

Port # 0, VLAN-ID # 3, Table-index 3
EoMPLS configured: 1
tag_rew_ptr = D0027B90
Leaf entry? = 1
```

```

FCR index = 20
 **tagrew_psa_addr = 0009EE40
 **tagrew_vir_addr = 7009EE40
 **tagrew_phy_addr = F009EE40
 [0-7] log 9400 mtu 4458 oq 4000 ai 8 oi 84000002 (encaps size 4)
 cw-size 4 vlanid-rew 2
 gather A30 (bufhdr size 32 EoMPLS (Control Word) Imposition profile 81)
 2 tag: 17 18
 counters 1182, 10 reported 1182, 10.
 Local OutputQ (Unicast): Slot:5 Port:0 RED queue:0 COS queue:0
 Output Q (Unicast): Port:0 RED queue:0 COS queue:0

```

## Configuring Per Subinterface MTU for Ethernet over MPLS

Cisco IOS Release 12.2(33)SRC introduces the ability to specify MTU values in xconnect subinterface configuration mode. When you use xconnect subinterface configuration mode to set the MTU value, you establish a pseudowire connection for situations where the interfaces have different MTU values that cannot be changed.

If you specify an MTU value in xconnect subinterface configuration mode that is outside the range of supported MTU values (64 bytes to the maximum number of bytes supported by the interface), the command might be rejected. If you specify an MTU value that is out of range in xconnect subinterface configuration mode, the router enters the command in subinterface configuration mode.

For example, if you specify an MTU of 1501 in xconnect subinterface configuration mode, and that value is out of range, the router enters the command in subinterface configuration mode, where it is accepted:

```

Router# configure terminal
router(config)# interface gigabitethernet0/2.1
router(config-subif)# xconnect 10.10.10.1 100 encapsulation mpls
router(config-subif-xconn)# mtu ?
<64 - 1500> MTU size in bytes
router(config-subif-xconn)# mtu 1501
router(config-subif)# mtu ?
<64 - 17940> MTU size in bytes

```

If the MTU value is not accepted in either xconnect subinterface configuration mode or subinterface configuration mode, then the command is rejected, as shown in the following example:

```

Router# configure terminal
router(config)# interface gigabitethernet0/2.1
router(config-subif)# xconnect 10.10.10.1 100 encapsulation mpls
router(config-subif-xconn)# mtu ?
<64 - 1500> MTU size in bytes
router(config-subif-xconn)# mtu 63
% Invalid input detected at ^ marker

```

## Restrictions

Configuring the MTU value in xconnect subinterface configuration mode has the following restrictions:

- The following features do not support MTU values in xconnect subinterface configuration mode:
  - Layer 2 Tunnel Protocol Version 3 (L2TPv3)
  - Virtual Private LAN services (VPLS)
  - L2VPN Pseudowire Switching
- The MTU value can be configured in xconnect subinterface configuration mode only on the following interfaces and subinterfaces:

- Ethernet
- FastEthernet
- GigabitEthernet
- The router uses an MTU validation process for remote VCs established through LDP, which compares the MTU value configured in xconnect subinterface configuration mode to the MTU value of the remote customer interface. If an MTU value has not been configured in xconnect subinterface configuration mode, then the validation process compares the MTU value of the local customer interface to the MTU value of the remote xconnect, either explicitly configured or inherited from the underlying interface or subinterface.
- When you configure the MTU value in xconnect subinterface configuration mode, the specified MTU value is not enforced by the dataplane. The dataplane enforces the MTU values of the interface (port mode) or subinterface (VLAN mode).
- Ensure that the interface MTU is larger than the MTU value configured in xconnect subinterface configuration mode. If the MTU value of the customer-facing subinterface is larger than the MTU value of the core-facing interface, traffic may not be able to travel across the pseudowire.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot / interface*
4. **mtu** *mtu-value*
5. **interface gigabitethernet** *slot / interface.subinterface*
6. **encapsulation dot1q** *vlan-id*
7. **xconnect** *peer-router-id vcid encapsulation mpls*
8. **mtu** *mtu-value*
9. **end**
10. **show mpls l2transport binding**

## DETAILED STEPS

|         | Command or Action                                                                                                                               | Purpose                                                                                                                                                                                                                           |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                 |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                  | Enters global configuration mode.                                                                                                                                                                                                 |
| Step 3  | <b>interface gigabitethernet slot/interface</b><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0                          | Specifies the Gigabit Ethernet interface and enters interface configuration mode.                                                                                                                                                 |
| Step 4  | <b>mtu mtu-value</b><br><br><b>Example:</b><br>Router(config-if)# mtu 2000                                                                      | Specifies the MTU value for the interface. The MTU value specified at the interface level can be inherited by a subinterface.                                                                                                     |
| Step 5  | <b>interface gigabitethernet slot /interface.subinterface</b><br><br><b>Example:</b><br>Router(config-if)# interface gigabitethernet4/0.1       | Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode.<br><br>Make sure the subinterface on the adjoining CE router is on the same VLAN as this PE router.                                       |
| Step 6  | <b>encapsulation dot1q vlan-id</b><br><br><b>Example:</b><br>Router(config-subif)# encapsulation dot1q 100                                      | Enables the subinterface to accept 802.1Q VLAN packets. The subinterfaces between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet. All other subinterfaces and backbone routers need not be. |
| Step 7  | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports. Enters xconnect subinterface configuration mode.                                                    |
| Step 8  | <b>mtu mtu-value</b><br><br><b>Example:</b><br>Router(config-if-xconn)# mtu 1400                                                                | Specifies the MTU for the VC.                                                                                                                                                                                                     |
| Step 9  | <b>end</b><br><br><b>Example:</b><br>Router(config-if-xconn)# end                                                                               | Exits xconnect subinterface configuration mode and returns to global configuration mode.                                                                                                                                          |
| Step 10 | <b>show mpls l2transport binding</b><br><br><b>Example:</b><br>Router# show mpls l2transport binding                                            | Displays the MTU values assigned to the local and remote interfaces.                                                                                                                                                              |

## Configuring Frame Relay over MPLS with DLCI-to-DLCI Connections

Frame Relay over MPLS encapsulates Frame Relay PDUs in MPLS packets and forwards them across the MPLS network. For Frame Relay, you can set up data-link connection identifier (DLCI)-to-DLCI connections or port-to-port connections. With DLCI-to-DLCI connections, the PE routers manipulate the packet by removing headers, adding labels, and copying control word elements from the header to the PDU.

Perform this task to configure Frame Relay over MPLS with DLCI-to-DLCI connections.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **frame-relay switching**
4. **interface serial** *slot / port*
5. **encapsulation frame-relay** [*cisco | ietf*]
6. **frame-relay intf-type dce**
7. **exit**
8. **connect** *connection-name interface dlci l2transport*
9. **xconnect** *peer-router-id vcid encapsulation mpls*

### DETAILED STEPS

|        | Command or Action                                                                                                                    | Purpose                                                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                       | Enters global configuration mode.                                                                                                                                                                         |
| Step 3 | <b>frame-relay switching</b><br><br><b>Example:</b><br>Router(config)# frame-relay switching                                         | Enables PVC switching on a Frame Relay device.                                                                                                                                                            |
| Step 4 | <b>interface serial</b> <i>slot/port</i><br><br><b>Example:</b><br>Router(config)# interface serial3/1                               | Specifies a serial interface and enters interface configuration mode.                                                                                                                                     |
| Step 5 | <b>encapsulation frame-relay</b> [ <i>cisco   ietf</i> ]<br><br><b>Example:</b><br>Router(config-if)# encapsulation frame-relay ietf | Specifies Frame Relay encapsulation for the interface. You can specify different types of encapsulations. You can set one interface to Cisco encapsulation and the other interface to IETF encapsulation. |

|        | Command or Action                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <pre>frame-relay intf-type dce</pre> <p><b>Example:</b><br/>Router(config-if)# frame-relay intf-type dce</p>                                                   | Specifies that the interface is a DCE switch. You can also specify the interface to support Network-to-Network Interface (NNI) and DTE connections.                                                                                                                                                                                                                                                                                                                                                                |
| Step 7 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                                                             | Exits from interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 8 | <pre>connect connection-name interface dlcil2transport</pre> <p><b>Example:</b><br/>Router(config)# connect fr1 serial5/0 1000 l2transport</p>                 | <p>Defines connections between Frame Relay PVCs and enters connect configuration submenu. Using the <b>l2transport</b> keyword specifies that the PVC will not be a locally switched PVC, but will be tunneled over the backbone network.</p> <p>The <i>connection-name</i> argument is a text string that you provide.</p> <p>The <i>interface</i> argument is the interface on which a PVC connection will be defined.</p> <p>The <i>dlci</i> argument is the DLCI number of the PVC that will be connected.</p> |
| Step 9 | <pre>xconnect peer-router-id vcid encapsulation mpls</pre> <p><b>Example:</b><br/>Router(config-fr-pw-switching)# xconnect 10.0.0.1 123 encapsulation mpls</p> | Creates the VC to transport the Layer 2 packets. In a DLCI-to-DLCI connection type, Frame Relay over MPLS uses the <b>xconnect</b> command in connect configuration submenu.                                                                                                                                                                                                                                                                                                                                       |

## Configuring Frame Relay over MPLS with Port-to-Port Connections

Frame Relay over MPLS encapsulates Frame Relay PDUs in MPLS packets and forwards them across the MPLS network. For Frame Relay, you can set up DLCI-to-DLCI connections or port-to-port connections. With port-to-port connections, you use HDLC mode to transport the Frame Relay encapsulated packets. In HDLC mode, the whole HDLC packet is transported. Only the HDLC flags and FCS bits are removed. The contents of the packet are not used or changed, including the backward explicit congestion notification (BECN), forward explicit congestion notification (FECN) and discard eligibility (DE) bits.

Perform this task to set up Frame Relay port-to-port connections.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serialslot/port**
4. **encapsulation hdlc**
5. **xconnect peer-router-id vcid encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                                                                                         | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                            | Enters global configuration mode.                                                                                |
| Step 3 | <b>interface serialslot/port</b><br><br><b>Example:</b><br>Router(config)# interface serial5/0                                                            | Specifies a serial interface and enters interface configuration mode.                                            |
| Step 4 | <b>encapsulation hdlc</b><br><br><b>Example:</b><br>Router(config-if)# encapsulation hdlc                                                                 | Specifies that Frame Relay PDUs will be encapsulated in HDLC packets.                                            |
| Step 5 | <b>xconnect peer-router-id vcid</b><br><b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123<br>encapsulation mpls | Creates the VC to transport the Layer 2 packets.                                                                 |

## Configuring HDLC and PPP over MPLS

With HDLC over MPLS, the whole HDLC packet is transported. The ingress PE router removes only the HDLC flags and FCS bits. The contents of the packet are not used or changed.

With PPP over MPLS, the ingress PE router removes the flags, address, control field, and the FCS.

### Restrictions

The following restrictions pertain to the HDLC over MPLS feature:

- Asynchronous interfaces are not supported.
- You must configure HDLC over MPLS on router interfaces only. You cannot configure HDLC over MPLS on subinterfaces.

The following restrictions pertain to the PPP over MPLS feature:

- Zero hops on one router is not supported. However, you can have back-to-back PE routers.
- Asynchronous interfaces are not supported. The connections between the CE and PE routers on both ends of the backbone must have similar link layer characteristics. The connections between the CE and PE routers must both be synchronous.
- Multilink PPP (MLP) is not supported.
- You must configure PPP on router interfaces only. You cannot configure PPP on subinterfaces.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serialslot/port**
4. **encapsulation encapsulation-type**
5. **xconnect peer-router-id vcid encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                | Purpose                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                   | Enters global configuration mode.                                                                                                                                                                |
| Step 3 | <b>interface serialslot/port</b><br><br><b>Example:</b><br>Router(config)# interface serial5/0                                                                                                   | Specifies a serial interface and enters interface configuration mode. You must configure HDLC and PPP over MPLS on router interfaces only. You cannot configure HDLC over MPLS on subinterfaces. |
| Step 4 | <b>encapsulation ppp</b><br>or<br><b>encapsulation hdlc</b><br><br><b>Example:</b><br>Router(config-if)# encapsulation ppp<br>or<br><br><b>Example:</b><br>Router(config-if)# encapsulation hdlc | Specifies HDLC or PPP encapsulation and enters connect configuration mode.                                                                                                                       |
| Step 5 | <b>xconnect peer-router-id vcid</b><br><b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-fr-pw-switching)# xconnect<br>10.0.0.1 123 encapsulation mpls                           | Creates the VC to transport the Layer 2 packets.                                                                                                                                                 |

## Configuring Tunnel Selection

The tunnel selection feature allows you to specify the path that traffic uses. You can specify either an MPLS TE tunnel or destination IP address or domain name server (DNS) name.

You also have the option of specifying whether the VCs should use the default path (the path LDP uses for signaling) if the preferred path is unreachable. This option is enabled by default; you must explicitly disable it.

You configure tunnel selection when you set up the pseudowire class. You enable tunnel selection with the **preferred-path** command. Then, you apply the pseudowire class to an interface that has been configured to transport AToM packets.

The following guidelines provide more information about configuring tunnel selection:

- The **preferred-path** command is available only if the pseudowire encapsulation type is MPLS.
- This tunnel selection feature is enabled when you exit from pseudowire submenu.
- The selected path should be an LSP destined to the peer PE router.
- The selected tunnel must be an MPLS TE tunnel.
- If you select a tunnel, the tunnel tailend must be on the remote PE router.
- If you specify an IP address, that address must be the IP address of the loopback interface on the remote PE router. The address must have a /32 mask. There must be an LSP destined to that selected address. The LSP need not be a TE tunnel.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**
5. **preferred-path** { **interface tunnel** *tunnel-number* | **peer** { *ip-address* | *host-name* } }  
[**disable-fallback**]
6. **exit**
7. **interface** *slot/port*
8. **encapsulation** *encapsulation-type*
9. **xconnect** *peer-router-id* *vcid* **pw-class** *name*

## DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                  |
| Step 3 | <b>pseudowire-class</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# pseudowire-class ts1 | Establishes a pseudowire class with a name that you specify and enters pseudowire configuration mode.              |

|        | Command or Action                                                                                                                                                                              | Purpose                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Step 4 | <p><b>encapsulation mpls</b></p> <p><b>Example:</b><br/>Router(config-pw)# encapsulation mpls</p>                                                                                              | Specifies the tunneling encapsulation. For AToM, the encapsulation type is <b>mpls</b> .                  |
| Step 5 | <p><b>preferred-path {interface tunnel tunnel-number   peer {ip-address   host-name}} [disable-fallback]</b></p> <p><b>Example:</b><br/>Router(config-pw)# preferred path peer 10.18.18.18</p> | Specifies the MPLS traffic engineering tunnel or IP address or hostname to be used as the preferred path. |
| Step 6 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config-pw)# exit</p>                                                                                                                          | Exits from pseudowire configuration mode.                                                                 |
| Step 7 | <p><b>interface slot/port</b></p> <p><b>Example:</b><br/>Router(config)# interface atm1/1</p>                                                                                                  | Specifies an interface and enters interface configuration mode.                                           |
| Step 8 | <p><b>encapsulation encapsulation-type</b></p> <p><b>Example:</b><br/>Router(config-if)# encapsulation aal5</p>                                                                                | Specifies the encapsulation for the interface.                                                            |
| Step 9 | <p><b>xconnect peer-router-id vcid pw-class name</b></p> <p><b>Example:</b><br/>Router(config-if)# xconnect 10.0.0.1 123 pw-class ts1</p>                                                      | Binds the attachment circuit to a pseudowire VC.                                                          |

## Examples

The following example sets up two preferred paths for PE1. One preferred path specifies an MPLS traffic engineering tunnel. The other preferred path specifies an IP address of a loopback address on PE2. There is a static route configured on PE1 that uses a TE tunnel to reach the IP address on PE2.

### PE1 Configuration

```

mpls label protocol ldp
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
pseudowire-class pw1
 encapsulation mpls
 preferred-path interface Tunnel1 disable-fallback
!
pseudowire-class pw2
 encapsulation mpls
 preferred-path peer 10.18.18.18
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 explicit name path-tu1
!
interface Tunnel2
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface gigabitethernet0/0/0
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 xconnect 10.16.16.16 101 pw-class pw1
!
interface ATM1/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
 encapsulation aal5
 xconnect 10.16.16.16 150 pw-class pw2
!
interface Ethernet2/0/1
 ip address 10.0.0.1 255.255.255.0

```

```

no ip directed-broadcast
tag-switching ip
mpls traffic-eng tunnels
ip rsvp bandwidth 15000 15000
!
router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.255 area 0
network 10.2.2.2 0.0.0.0 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
!
ip route 10.18.18.18 255.255.255.255 Tunnel2
!
ip explicit-path name path-tul enable
next-address 10.0.0.1
index 3 next-address 10.0.0.1

```

### PE2 Configuration

```

mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback0
interface Loopback0
ip address 10.16.16.16 255.255.255.255
no ip directed-broadcast
no ip mroute-cache
!
interface Loopback2
ip address 10.18.18.18 255.255.255.255
no ip directed-broadcast
!
interface Ethernet3/1
ip address 10.0.0.2 255.255.255.0
no ip directed-broadcast
mpls traffic-eng tunnels
mpls ip
no cdp enable
ip rsvp bandwidth 15000 15000
!
interface Ethernet3/3
no ip address
no ip directed-broadcast
no cdp enable
!
interface Ethernet3/3.1
encapsulation dot1Q 222
no ip directed-broadcast
no cdp enable
mpls l2transport route 10.2.2.2 101
!
interface ATM5/0
no ip address
no ip directed-broadcast
no atm enable-ilmi-trap
no atm ilmi-keepalive
pvc 0/50 l2transport
encapsulation aal5
xconnect 10.2.2.2 150 encapsulation mpls
!
router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.255 area 0
network 10.16.16.16 0.0.0.0 area 0

```

```
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
```

In the following example, the **show mpls l2transport vc** command shows the following information about the VCs:

- VC 101 has been assigned a preferred path called Tunnel1. The default path is disabled, because the preferred path specified that the default path should not be used if the preferred path fails.
- VC 150 has been assigned an IP address of a loopback address on PE2. The default path can be used if the preferred path fails.

In the following example, command output that is bolded shows the preferred path information.

```
Router# show mpls l2transport vc detail

Local interface: Gi0/0/0.1 up, line protocol up, Eth VLAN 222 up
 Destination address: 10.16.16.16, VC ID: 101, VC status: up
 Preferred path: Tunnel1, active
 Default path: disabled
 Tunnel label: 3, next hop point2point
 Output interface: Tu1, imposed label stack {17 16}
 Create time: 00:27:31, last status change time: 00:27:31
 Signaling protocol: LDP, peer 10.16.16.16:0 up
 MPLS VC labels: local 25, remote 16
 Group ID: local 0, remote 6
 MTU: local 1500, remote 1500
 Remote interface description:
 Sequencing: receive disabled, send disabled
 VC statistics:
 packet totals: receive 10, send 10
 byte totals: receive 1260, send 1300
 packet drops: receive 0, send 0

Local interface: AT1/0/0 up, line protocol up, ATM AAL5 0/50 up
 Destination address: 10.16.16.16, VC ID: 150, VC status: up
 Preferred path: 10.18.18.18, active
 Default path: ready
 Tunnel label: 3, next hop point2point
 Output interface: Tu2, imposed label stack {18 24}
 Create time: 00:15:08, last status change time: 00:07:37
 Signaling protocol: LDP, peer 10.16.16.16:0 up
 MPLS VC labels: local 26, remote 24
 Group ID: local 2, remote 0
 MTU: local 4470, remote 4470
 Remote interface description:
 Sequencing: receive disabled, send disabled
 VC statistics:
 packet totals: receive 0, send 0
 byte totals: receive 0, send 0
 packet drops: receive 0, send 0
```

## Troubleshooting Tips

You can use the **debug mpls l2transport vc event** command to troubleshoot tunnel selection. For example, if the tunnel interface that is used for the preferred path is shut down, the default path is enabled. The **debug mpls l2transport vc event** command provides the following output:

```
AToM SMGR [10.2.2.2, 101]: Processing imposition update, vc_handle 62091860, update_action
3, remote_vc_label 16
AToM SMGR [10.2.2.2, 101]: selected route no parent rewrite: tunnel not up
AToM SMGR [10.2.2.2, 101]: Imposition Programmed, Output Interface: Et3/2
```

## Setting Experimental Bits with AToM

MPLS AToM uses the three experimental bits in a label to determine the queue of packets. You statically set the experimental bits in both the VC label and the LSP tunnel label, because the LSP tunnel label might be removed at the penultimate router. The following sections explain the transport-specific implementations of the EXP bits.



### Note

For information about setting EXP bits on the Cisco 12000 series router for Cisco IOS Release 12.0(30)S, see the *AToM: L2 QoS* feature module.

For configuration steps and examples, see the [“Setting Experimental Bits with AToM” section on page 70](#).

## Restrictions

The following restrictions apply to ATM AAL5 over MPLS with EXP bits:

- ATM AAL5 over MPLS allows you to statically set the experimental bits.
- If you do not assign values to the experimental bits, the priority bits in the header’s “tag control information” field are set to zero.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

The following restrictions apply to ATM Cell Relay over MPLS with EXP bits:

- ATM Cell Relay over MPLS allows you to statically set the experimental bits in VC, PVP, and port modes.
- If you do not assign values to the experimental bits, the priority bits in the header’s “tag control information” field are set to zero.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

The following restrictions apply to Ethernet over MPLS with EXP bits:

### On the Cisco 7200 and 7500 Series Routers

- Ethernet over MPLS allows you to set the EXP bits by using either of the following methods:
  - Writing the priority bits into the experimental bit field, which is the default.
  - Using the **match any** command with the **set mpls exp** command.
- If you do not assign values to the experimental bits, the priority bits in the 802.1Q header’s “tag control information” field are written into the experimental bit fields.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

### On the Cisco 10720 Internet Router

[Table 7](#) lists the commands that are supported on the Cisco 10720 Internet router for Ethernet over MPLS. The letter Y means that the command is supported on that interface. A dash (—) means that command is not supported on that interface.

**Note**

The **match cos** command is supported only on subinterfaces, not main interfaces.

**Table 7** *Commands Supported on the Cisco 10720 Router for Ethernet over MPLS*

| Commands                         | Imposition |     | Disposition |     |
|----------------------------------|------------|-----|-------------|-----|
|                                  | In         | Out | In          | Out |
| <b>Traffic Matching Commands</b> |            |     |             |     |
| <b>match any</b>                 | Y          | Y   | Y           | Y   |
| <b>match cos</b>                 | Y          | —   | —           | —   |
| <b>match input-interface</b>     | —          | —   | Y           | Y   |
| <b>match mpls exp</b>            | —          | Y   | Y           | —   |
| <b>match qos-group</b>           | —          | Y   | —           | Y   |
| <b>Traffic Action Commands</b>   |            |     |             |     |
| <b>set cos</b>                   | —          | —   | —           | Y   |
| <b>set mpls exp</b>              | Y          | —   | —           | —   |
| <b>set qos-group</b>             | Y          | —   | Y           | —   |
| <b>set srp-priority</b>          | —          | Y   | —           | —   |

The following restrictions apply to Frame Relay over MPLS and EXP bits:

- If you do not assign values to the experimental bits, the priority bits in the header's "tag control information" field are set to zero.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

The following restrictions apply to HDLC over MPLS and PPP over MPLS and EXP bits:

- If you do not assign values to the experimental bits, zeros are written into the experimental bit fields.
- On the Cisco 7500 series routers, enable distributed Cisco Express Forwarding before setting the experimental bits.

Set the experimental bits in both the VC label and the LSP tunnel label. You set the experimental bits in the VC label, because the LSP tunnel label might be removed at the penultimate router. Perform this task to set the experimental bits.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-name*
4. **match any**
5. **policy-map** *policy-name*
6. **class** *class-name*
7. **set mpls experimental** *value*
8. **exit**

9. **exit**
10. **interface** *slot/port*
11. **service-policy input** *policy-name*
12. **exit**
13. **exit**
14. **show policy-map interface** *interface-name* [**vc** [*vpi/l*] *vci*] [**dlei** *dlei*] [**input** | **output**]

## DETAILED STEPS

|        | Command or Action                                                                                                     | Purpose                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                        | Enters global configuration mode.                                                                                                                                                                        |
| Step 3 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map class1                         | Specifies the user-defined name of the traffic class and enters class map configuration mode.                                                                                                            |
| Step 4 | <b>match any</b><br><br><b>Example:</b><br>Router(config-cmap)# match any                                             | Specifies that all packets will be matched. Use only the <b>any</b> keyword. Other keywords might cause unexpected results.                                                                              |
| Step 5 | <b>policy-map</b> <i>policy-name</i><br><br><b>Example:</b><br>Router(config-cmap)# policy-map policy1                | Specifies the name of the traffic policy to configure and enters policy-map configuration mode.                                                                                                          |
| Step 6 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-pmap)# class class1                            | Specifies the name of a predefined traffic class, which was configured with the <b>class-map</b> command, used to classify traffic to the traffic policy and enters policy-map class configuration mode. |
| Step 7 | <b>set mpls experimental</b> <i>value</i><br><br><b>Example:</b><br>Router(config-pmap-c)# set mpls experimental<br>7 | Designates the value to which the MPLS bits are set if the packets match the specified policy map.                                                                                                       |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap-c)# exit                                                     | Exits policy-map class configuration mode.                                                                                                                                                               |

|         | Command or Action                                                                                                                                                  | Purpose                                                          |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap)# exit                                                                                                    | Exits policy-map configuration mode.                             |
| Step 10 | <b>interface slot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm4/0                                                                              | Specifies the interface and enters interface configuration mode. |
| Step 11 | <b>service-policy input policy-name</b><br><br><b>Example:</b><br>Router(config-if)# service-policy input policy1                                                  | Attaches a traffic policy to an interface.                       |
| Step 12 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                      | Exits interface configuration mode.                              |
| Step 13 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                         | Exits global configuration mode.                                 |
| Step 14 | <b>show policy-map interface interface-name [vc [vpi/] vci] [dlci dlci] [input   output]</b><br><br><b>Example:</b><br>Router# show policy-map interface serial3/0 | Displays the traffic policy attached to an interface.            |

## Setting the Frame Relay Discard Eligibility Bit on the Cisco 7200 and 7500 Series Routers

You can use the DE bit in the address field of a Frame Relay frame to prioritize frames in congested Frame Relay networks. The Frame Relay DE bit has only one bit and can therefore only have two settings, 0 or 1. If congestion occurs in a Frame Relay network, frames with the DE bit set to 1 are discarded before frames with the DE bit set to 0. Therefore, important traffic should have the DE bit set to 0, and less important traffic should be forwarded with the DE bit set at 1. The default DE bit setting is 0. You can change the DE bit setting to 1 with the **set fr-de** command.



### Note

The **set fr-de** command can be used only in an output service policy.

Perform this task to set the Frame Relay DE bit on the Cisco 7200 and 7500 series routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **policy-map** *policy-name*
4. **class** *class-name*
5. **set fr-de**

## DETAILED STEPS

|        | Command or Action                                                                                 | Purpose                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                    | Enters global configuration mode.                                                                                                                     |
| Step 3 | <b>policy-map</b> <i>policy-name</i><br><br><b>Example:</b><br>Router(config)# policy-map policy1 | Specifies the name of the traffic policy to configure and enters policy-map configuration mode. Names can be a maximum of 40 alphanumeric characters. |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-pmap)# class class1        | Specifies the name of a predefined traffic class and enters policy-map class configuration mode.                                                      |
| Step 5 | <b>set fr-de</b><br><br><b>Example:</b><br>Router(config-pmap-c)# set fr-de                       | Sets the Frame Relay DE bit setting for all packets that match the specified traffic class from 0 to 1.                                               |

## Examples

The following example shows how to configure the service policy called set-de and attach it to an interface. In this example, the class map called data evaluates all packets exiting the interface for an IP precedence value of 1. If the exiting packet has been marked with the IP precedence value of 1, the packet's DE bit is set to 1.

```
class-map data
match ip precedence 1

policy-map set-de
class data
set fr-de
interface Serial0/0/0
encapsulation frame-relay
interface Serial0/0/0.1 point-to-point
ip address 192.168.249.194 255.255.255.252
frame-relay interface-dlci 100
service output set-de
```

## Matching the Frame Relay DE Bit on the Cisco 7200 and 7500 Series Routers

You can use the **match fr-de** command to enable frames with a DE bit setting of 1 to be considered a member of a defined class and forwarded according to the specifications set in the service policy.

Perform this task to match frames with the FR DE bit set to 1.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match fr-de**

### DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                  |
| Step 3 | <b>class-map</b> <i>class-map-name</i><br><br><b>Example:</b><br>Router(config)# class-map de-bits | Specifies the name of a predefined traffic class and enters class-map configuration mode.                          |
| Step 4 | <b>match fr-de</b><br><br><b>Example:</b><br>Router(config-cmap)# match fr-de                      | Classifies all frames with the DE bit set to 1.                                                                    |

### Examples

The following example shows how to configure the service policy called match-de and attach it to an interface. In this example, the class map called data evaluates all packets entering the interface for a DE bit setting of 1. If the entering packet has been a DE bit value of 1, the packet's EXP bit setting is set to 3.

```
class-map data
match fr-de
policy-map match-de
class data
set mpls exp 3
ip routing
ip cef distributed
mpls label protocol ldp
interface Loopback0
```

```

ip address 10.20.20.20 255.255.255.255
interface Ethernet1/0/0
ip address 10.0.0.2 255.255.255.0
mpls ip
interface Serial4/0/0
encapsulation frame-relay
service input match-de
connect 100 Serial4/0/0 100 l2transport
xconnect 10.10.10.10 100 encapsulation mpls

```

## Configuration Examples for Any Transport over MPLS

This section contains the following configuration examples:

- [ATM over MPLS: Example, page 76](#)
- [Ethernet over MPLS with MPLS Traffic Engineering Fast Reroute: Example, page 76](#)
- [Configuring Per Subinterface MTU for Ethernet over MPLS: Example, page 79](#)
- [Configuring MTU Values in xconnect Configuration Mode for L2VPN Interworking: Example, page 81](#)

### ATM over MPLS: Example

[Example 1](#) shows the configuration of ATM over MPLS on two PE routers.

#### *Example 1 ATM over MPLS Configuration Example*

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                      | PE2                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.16.12.12 255.255.255.255 ! interface ATM4/0 pvc 0/100 l2transport encapsulation aal0 xconnect 10.13.13.13 100 encapsulation mpls ! interface ATM4/0.300 point-to-point no ip directed-broadcast no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 xconnect 10.13.13.13 300 encapsulation mpls </pre> | <pre> mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.13.13.13 255.255.255.255 ! interface ATM4/0 pvc 0/100 l2transport encapsulation aal0 xconnect 10.16.12.12 100 encapsulation mpls ! interface ATM4/0.300 point-to-point no ip directed-broadcast no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 xconnect 10.16.12.12 300 encapsulation mpls </pre> |

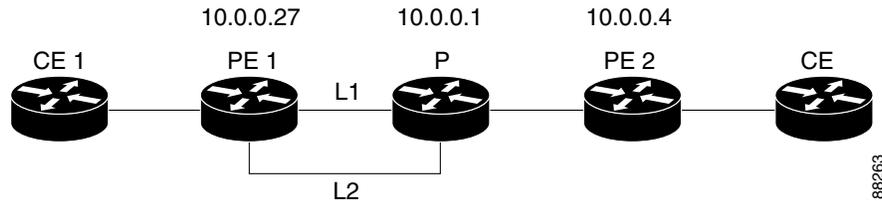
### Ethernet over MPLS with MPLS Traffic Engineering Fast Reroute: Example

The following configuration example and [Figure 2](#) show the configuration of Ethernet over MPLS with fast reroute on AToM PE routers.

Routers PE1 and PE2 have the following characteristics:

- A TE tunnel called Tunnel41 is configured between PE1 and PE2, using an explicit path through a link called L1. AToM VCs are configured to travel through the FRR-protected tunnel Tunnel41.
- The link L1 is protected by FRR, the backup tunnel is Tunnel1.
- PE2 is configured to forward the AToM traffic back to PE1 through the L2 link.

**Figure 2 Fast Reroute Configuration**



### PE1 Configuration

```

mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
pseudowire-class T41
 encapsulation mpls
 preferred-path interface Tunnel41 disable-fallback
!
pseudowire-class IP1
 encapsulation mpls
 preferred-path peer 10.4.0.1 disable-fallback
!
interface Loopback1
 ip address 10.0.0.27 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel destination 10.0.0.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 10000
 tunnel mpls traffic-eng path-option 1 explicit name FRR
!
interface Tunnel41
 ip unnumbered Loopback1
 tunnel destination 10.0.0.4
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name name-1
 tunnel mpls traffic-eng fast-reroute
!
interface POS0/0
 description pelname POS8/0/0
 ip address 10.1.0.2 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 crc 16
 clock source internal
 pos ais-shut
 pos report lrldi
 ip rsvp bandwidth 155000 155000
!
interface POS0/3

```

```

description pelname POS10/1/0
ip address 10.1.0.14 255.255.255.252
mpls traffic-eng tunnels
crc 16
clock source internal
ip rsvp bandwidth 155000 155000
!
interface gigabitethernet3/0.1
encapsulation dot1Q 203
xconnect 10.0.0.4 2 pw-class IP1
!
interface gigabitethernet3/0.2
encapsulation dot1Q 204
xconnect 10.0.0.4 4 pw-class T41
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0
!
ip classless
ip route 10.4.0.1 255.255.255.255 Tunnel41
!
ip explicit-path name xxxx-1 enable
next-address 10.4.1.2
next-address 10.1.0.10

```

### P Configuration

```

ip cef
mpls traffic-eng tunnels
!
interface Loopback1
ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet1/0/0
ip address 10.4.1.2 255.255.255.0
mpls traffic-eng tunnels
ip rsvp bandwidth 10000 10000
!
interface POS8/0/0
description xxxx POS0/0
ip address 10.1.0.1 255.255.255.252
mpls traffic-eng tunnels
pos ais-shut
pos report lrldi
ip rsvp bandwidth 155000 155000
!
interface POS10/1/0
description xxxx POS0/3
ip address 10.1.0.13 255.255.255.252
mpls traffic-eng tunnels
ip rsvp bandwidth 155000 155000
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

```

### PE2 Configuration

```

ip cef
mpls label protocol ldp
mpls traffic-eng tunnels

```

```

mpls ldp router-id Loopback1 force
!
interface Loopback1
 ip address 10.0.0.4 255.255.255.255
!
interface loopback 2
 ip address 10.4.0.1 255.255.255.255
!
interface Tunnel27
 ip unnumbered Loopback1
 tunnel destination 10.0.0.27
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name xxxx-1
!
interface FastEthernet0/0.2
 encapsulation dot1Q 203
 xconnect 10.0.0.27 2 encapsulation mpls
!
interface FastEthernet0/0.3
 encapsulation dot1Q 204
 xconnect 10.0.0.27 4 encapsulation mpls
!
interface FastEthernet1/1
 ip address 10.4.1.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10

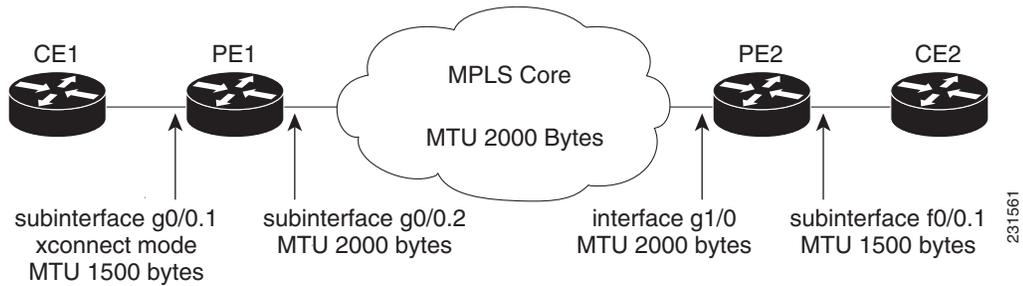
```

## Configuring Per Subinterface MTU for Ethernet over MPLS: Example

Figure 3 shows a configuration that enables matching MTU values between VC endpoints.

As shown in Figure 3, PE1 is configured in xconnect subinterface configuration mode with an MTU value of 1500 bytes in order to establish an end-to-end VC with PE2, which also has an MTU value of 1500 bytes. If PE1 was not set with an MTU value of 1500 bytes, in xconnect subinterface configuration mode, the subinterface would inherit the MTU value of 2000 bytes set on the interface. This would cause a mismatch in MTU values between the VC endpoints, and the VC would not come up.

**Figure 3** Configuring MTU Values in xconnect Subinterface Configuration Mode



The following examples show the router configurations in [Figure 3](#):

#### CE1 configuration

```
interface gigabitethernet0/0
 mtu 1500
 no ip address
!
interface gigabitethernet0/0.1
 encapsulation dot1Q 100
 ip address 10.181.182.1 255.255.255.0
```

#### PE1 configuration

```
interface gigabitethernet0/0
 mtu 2000
 no ip address
!
interface gigabitethernet0/0.1
 encapsulation dot1Q 100
 xconnect 10.1.1.152 100 encapsulation mpls
 mtu 1500
!
interface gigabitethernet0/0.2
 encapsulation dot1Q 200
 ip address 10.151.100.1 255.255.255.0
 mpls ip
```

#### PE2 configuration

```
interface gigabitethernet1/0
 mtu 2000
 no ip address
!
interface gigabitethernet1/0.2
 encapsulation dot1Q 200
 ip address 10.100.152.2 255.255.255.0
 mpls ip
!
interface fastethernet0/0
 no ip address
!
interface fastethernet0/0.1
 description default MTU of 1500 for FastEthernet
 encapsulation dot1Q 100
 xconnect 10.1.1.151 100 encapsulation mpls
```

**CE2 configuration**

```
interface fastethernet0/0
 no ip address
interface fastethernet0/0.1
 encapsulation dot1Q 100
 ip address 10.181.182.2 255.255.255.0
```

The **show mpls l2transport binding** command, issued from router PE1, shows a matching MTU value of 1500 bytes on both the local and remote routers:

```
Router# show mpls l2transport binding
```

```
Destination Address: 10.1.1.152, VC ID: 100
Local Label: 100
 Cbit: 1, VC Type: Ethernet, GroupID: 0
 MTU: 1500, Interface Desc: n/a
 VCCV: CC Type: CW [1], RA [2]
 CV Type: LSPV [2]
Remote Label: 202
 Cbit: 1, VC Type: Ethernet, GroupID: 0
 MTU: 1500, Interface Desc: n/a
 VCCV: CC Type: RA [2]
 CV Type: LSPV [2]
```

```
Router# show mpls l2transport vc detail
```

```
Local interface: Gi0/0.1 up, line protocol up, Eth VLAN 100 up
Destination address: 10.1.1.152, VC ID: 100, VC status: up
Output interface: Gi0/0.2, imposed label stack {202}
Preferred path: not configured
Default path: active
Next hop: 10.151.152.2
Create time: 1d11h, last status change time: 1d11h
Signaling protocol: LDP, peer 10.1.1.152:0 up
Targeted Hello: 10.1.1.151(LDP ID) -> 10.1.1.152
MPLS VC labels: local 100, remote 202
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
 packet totals: receive 41, send 39
 byte totals: receive 4460, send 5346
 packet drops: receive 0, send 0
```

## Configuring MTU Values in xconnect Configuration Mode for L2VPN Interworking: Example

The following example shows an L2VPN Interworking example. The PE1 router has a serial interface configured with an MTU value of 1492 bytes. The PE2 router uses xconnect configuration mode to set a matching MTU of 1492 bytes, which allows the two routers to form an interworking VC. If the PE2 router did not set the MTU value in xconnect configuration mode, the interface would be set to 1500 bytes by default and the VC would not come up.

**PE1 Configuration**

```
pseudowire-class atom-ipiw
 encapsulation mpls
 interworking ip
```

```

!
interface Loopback0
 ip address 10.1.1.151 255.255.255.255
!
interface Serial2/0
 mtu 1492
 no ip address
 encapsulation ppp
 no fair-queue
 serial restart-delay 0
 xconnect 10.1.1.152 123 pw-class atom-ipiw
!
interface Serial4/0
 ip address 10.151.100.1 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.151 0.0.0.0 area 0
 network 10.151.100.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0

```

### PE2 Configuration

```

pseudowire-class atom-ipiw
 encapsulation mpls
 interworking ip
!
interface Loopback0
 ip address 10.1.1.152 255.255.255.255
!
interface Ethernet0/0
 no ip address
 xconnect 10.1.1.151 123 pw-class atom-ipiw
 mtu 1492
!
interface Serial4/0
 ip address 10.100.152.2 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.152 0.0.0.0 area 0
 network 10.100.152.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0

```

The **show mpls l2transport binding** command shows that the MTU value for the local and remote routers is 1492 bytes.

### PE1

```
Router# show mpls l2transport binding
```

```

Destination Address: 10.1.1.152, VC ID: 123
Local Label: 105
 Cbit: 1, VC Type: PPP, GroupID: 0
 MTU: 1492, Interface Desc: n/a
 VCCV: CC Type: CW [1], RA [2]

```

```

CV Type: LSPV [2]
Remote Label: 205
 Cbit: 1, VC Type: Ethernet, GroupID: 0
 MTU: 1492, Interface Desc: n/a
 VCCV: CC Type: RA [2]
 CV Type: LSPV [2]

```

Router# **show mpls l2transport vc detail**

```

Local interface: Se2/0 up, line protocol up, PPP up
MPLS VC type is PPP, interworking type is IP
Destination address: 10.1.1.152, VC ID: 123, VC status: up
Output interface: Se4/0, imposed label stack {1003 205}
Preferred path: not configured
Default path: active
Next hop: point2point
Create time: 00:25:29, last status change time: 00:24:54
Signaling protocol: LDP, peer 10.1.1.152:0 up
Targeted Hello: 10.1.1.151(LDP Id) -> 10.1.1.152
Status TLV support (local/remote) : enabled/supported
Label/status state machine : established, LruRru
Last local dataplane status rcvd: no fault
Last local SSS circuit status rcvd: no fault
Last local SSS circuit status sent: no fault
Last local LDP TLV status sent: no fault
Last remote LDP TLV status rcvd: no fault
MPLS VC labels: local 105, remote 205
Group ID: local n/a, remote 0
MTU: local 1492, remote 1492
Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
packet totals: receive 30, send 29
byte totals: receive 2946, send 3364
packet drops: receive 0, send 0

```

## PE2

Router# **show mpls l2transport binding**

```

Destination Address: 10.1.1.151, VC ID: 123
Local Label: 205
 Cbit: 1, VC Type: Ethernet, GroupID: 0
 MTU: 1492, Interface Desc: n/a
 VCCV: CC Type: RA [2]
 CV Type: LSPV [2]
Remote Label: 105
 Cbit: 1, VC Type: Ethernet, GroupID: 0
 MTU: 1492, Interface Desc: n/a
 VCCV: CC Type: CW [1], RA [2]
 CV Type: LSPV [2]

```

Router# **show mpls l2transport vc detail**

```

Local interface: Et0/0 up, line protocol up, Ethernet up
MPLS VC type is Ethernet, interworking type is IP
Destination address: 10.1.1.151, VC ID: 123, VC status: up
Output interface: Se4/0, imposed label stack {1002 105}
Preferred path: not configured
Default path: active
Next hop: point2point
Create time: 00:25:19, last status change time: 00:25:19
Signaling protocol: LDP, peer 10.1.1.151:0 up
Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151

```

```

Status TLV support (local/remote) : enabled/supported
Label/status state machine : established, LruRru
Last local dataplane status rcvd: no fault
Last local SSS circuit status rcvd: no fault
Last local SSS circuit status sent: no fault
Last local LDP TLV status sent: no fault
Last remote LDP TLV status rcvd: no fault
MPLS VC labels: local 205, remote 105
Group ID: local n/a, remote 0
MTU: local 1492, remote 1492
Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
packet totals: receive 29, send 30
byte totals: receive 2900, send 3426
packet drops: receive 0, send 0

```

## Additional References

The following sections provide references related to the Any Transport over MPLS feature.

## Related Documents

| Related Topic                                                                                                                                                          | Document Title                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Any Transport over MPLS                                                                                                                                                | Overview section of <a href="#">Cisco Any Transport over MPLS</a>                                          |
| Any Transport over MPLS for the Cisco 10000 series router                                                                                                              | <a href="#">Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide</a> |
| Layer 2 Tunnel Protocol Version 3 (L2TPv3): Provides the ability to tunnel any Layer 2 payload over an IP core network using Layer 2 virtual private networks (L2VPNs) | <a href="#">Layer 2 Tunnel Protocol Version 3 (L2TPv3)</a>                                                 |
| L2VPN interworking                                                                                                                                                     | <a href="#">L2VPN interworking</a>                                                                         |

## Standards

| Standard                                  | Title                                                                           |
|-------------------------------------------|---------------------------------------------------------------------------------|
| draft-martini-l2circuit-trans-mpls-08.txt | <a href="#">Transport of Layer 2 Frames Over MPLS</a>                           |
| draft-martini-l2circuit-encap-mpls-04.txt | <a href="#">Encapsulation Methods for Transport of Layer 2 Frames Over MPLS</a> |

## MIBs

| MIB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | MIBs Link                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ATM AAL5 over MPLS and ATM Cell Relay over MPLS:</p> <ul style="list-style-type: none"> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> <li>• ATM MIB (ATM-MIB.my)</li> <li>• CISCO AAL5 MIB (CISCO-AAL5-MIB.my)</li> <li>• Cisco Enterprise ATM Extension MIB (CISCO-ATM-EXT-MIB.my)</li> <li>• Supplemental ATM Management Objects (CISCO-IETF-ATM2-PVCTRAP-MIB.my)</li> <li>• Interfaces MIB (IF-MIB.my)</li> </ul> <p>Ethernet over MPLS</p> <ul style="list-style-type: none"> <li>• CISCO-ETHERLIKE-CAPABILITIES.my</li> <li>• Ethernet MIB (ETHERLIKE-MIB.my)</li> <li>• Interfaces MIB (IF-MIB.my)</li> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> </ul> <p>Frame Relay over MPLS</p> <ul style="list-style-type: none"> <li>• Cisco Frame Relay MIB (CISCO-FRAME-RELAY-MIB.my)</li> <li>• Interfaces MIB (IF-MIB.my)</li> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> </ul> <p>HDLC and PPP over MPLS</p> <ul style="list-style-type: none"> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> <li>• Interface MIB (IF-MIB.my)</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://tools.cisco.com/go/mibs">http://tools.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title                            |
|----------|----------------------------------|
| RFC 3032 | <i>MPLS Label Stack Encoding</i> |
| RFC 3036 | <i>LDP Specification</i>         |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                       | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **cell-packing**
- **encapsulation (Any Transport over MPLS)**
- **oam-ac emulation-enable**

## Feature Information for Any Transport over MPLS

[Table 8](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

[Table 8](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 8** Feature Information for Any Transport over MPLS

| Feature Name            | Releases   | Feature Information                                                                           |
|-------------------------|------------|-----------------------------------------------------------------------------------------------|
| Any Transport over MPLS | 12.0(10)ST | Any Transport over MPLS: ATM AAL5 over MPLS was introduced on the Cisco 12000 series routers. |

**Table 8**      **Feature Information for Any Transport over MPLS (continued)**

| Feature Name | Releases   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.1(8a)E  | In 12.1(8a)E, Ethernet over MPLS was introduced on the Cisco 7600 series Internet router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|              | 12.0(21)ST | Any Transport over MPLS: Ethernet over MPLS was introduced on the Cisco 12000 series routers. ATM AAL5 over MPLS was updated.                                                                                                                                                                                                                                                                                                                                                                                                                              |
|              | 12.0(22)S  | In 12.0(22)S, Ethernet over MPLS was integrated into this release. Support for the Cisco 10720 Internet router was added. ATM AAL5 over MPLS was integrated into this release for the Cisco 12000 series routers.                                                                                                                                                                                                                                                                                                                                          |
|              | 12.0(23)S  | In 12.0(23)S, the following new features were introduced: <ul style="list-style-type: none"> <li>• ATM Cell Relay over MPLS (single cell relay, VC mode)</li> <li>• Frame Relay over MPLS</li> <li>• HDLC over MPLS</li> <li>• PPP over MPLS</li> </ul> <p>These features were supported on the Cisco 7200 and 7500 series routers.</p> <p>The Cisco 12000, 7200, and 7500 series routers added support for the following features:</p> <ul style="list-style-type: none"> <li>• ATM AAL5 over MPLS</li> <li>• Ethernet over MPLS (VLAN mode)</li> </ul>   |
|              | 12.2(14)S  | The AToM features were integrated into Cisco IOS Release 12.2(14)S.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|              | 12.2(15)T  | The AToM features were integrated into Cisco IOS Release 12.2(15)T.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|              | 12.0(25)S  | In 12.0(25)S, the following new features were introduced: <ul style="list-style-type: none"> <li>• New commands for configuring AToM</li> <li>• Ethernet over MPLS: port mode</li> <li>• ATM Cell Relay over MPLS: packed cell relay</li> <li>• ATM Cell Relay over MPLS: VP mode</li> <li>• ATM Cell Relay over MPLS: port mode</li> <li>• Distributed Cisco Express Forwarding mode for Frame Relay, PPP, and HDLC over MPLS</li> <li>• Fast reroute with AToM</li> <li>• Tunnel selection</li> <li>• Traffic policing</li> <li>• QoS support</li> </ul> |
|              | 12.0(26)S  | In 12.0(26)S, the following new features were introduced: <ul style="list-style-type: none"> <li>• Support for connecting disparate attachment circuits. See <i>L2VPN Interworking</i> for more information.</li> <li>• QoS functionality with AToM for the Cisco 7200 series routers.</li> <li>• Support for FECN and BECN marking with Frame Relay over MPLS. (See <i>BECN and FECN Marking for Frame Relay over MPLS</i> for more information.)</li> </ul>                                                                                              |

Table 8 Feature Information for Any Transport over MPLS (continued)

| Feature Name | Releases   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.0(27)S  | In 12.0(27)S, the following new features were introduced: <ul style="list-style-type: none"> <li>ATM Cell Relay over MPLS: Packed Cell Relay for VC, PVP, and port mode for the Cisco 12000 series router.</li> <li>Support for ATM over MPLS on the Cisco 12000 series 4-port OC-12X/STM-4 ATM ISE line card.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|              | 12.2(25)S  | This feature was integrated into Cisco IOS Release 12.2(25)S for the Cisco 7200 and 7500 series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|              | 12.0(29)S  | In 12.0(29)S, the “Any Transport over MPLS Sequencing Support” feature was added for the Cisco 7200 and 7500 series routers. See the <a href="#">Any Transport over MPLS (AToM) Sequencing Support</a> document for more information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|              | 12.0(30)S  | In 12.0(30)S, the following new features were introduced: <ul style="list-style-type: none"> <li>ATM VC Class Support—You can specify AAL5 and AAL0 encapsulations as part of a VC class. You can also enable cell packing and OAM emulation as part of a VC class. A VC class can be attached to an interface, subinterface, or VC. See the “<a href="#">How to Configure Any Transport over MPLS</a>” section on page 14 for links to the sections that explain the ATM VC Class Support feature.</li> <li>VLAN ID Rewrite—This feature was enhanced to enable the IP Service Engine (ISE) 4-port Gigabit Ethernet line card to perform VLAN ID rewrite at both the imposition and disposition sides of the edge-facing router. See the “<a href="#">Configuring Ethernet over MPLS with VLAN ID Rewrite</a>” section on page 53 for more information.</li> </ul> |
|              | 12.0(31)S  | In 12.0(31)S, the Cisco 12000 series router introduced the following enhancements: <ul style="list-style-type: none"> <li>AToM VC Independence—With this enhancement, fast reroute is accomplished in less than 50 milliseconds, regardless of the number of VCs configured. See the “<a href="#">MPLS Traffic Engineering Fast Reroute</a>” section on page 6 for more information.</li> <li>Support for ISE line cards on the 2.5G ISE SPA Interface Processor (SIP).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |
|              | 12.0(32)S  | In 12.0(32)S, the Cisco 12000 series router added engine 5 line card support for the following transport types: <ul style="list-style-type: none"> <li>Ethernet over MPLS</li> <li>Frame Relay over MPLS</li> <li>HDLC over MPLS</li> <li>PPP over MPLS</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|              | 12.2(28)SB | This feature was integrated into Cisco IOS Release 12.2(28)SB on the Cisco 10000 series routers. Platform-specific configuration information is contained in the “Configuring Any Transport over MPLS” section of the <a href="#">Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 8**      **Feature Information for Any Transport over MPLS (continued)**

| Feature Name | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.4(11)T   | <p>Any Transport over MPLS was integrated into Cisco IOS Release 12.4(11)T and supports the following features:</p> <ul style="list-style-type: none"> <li>• Any Transport over MPLS: Ethernet over MPLS: Port Mode</li> <li>• Any Transport over MPLS: Ethernet over MPLS: VLAN Mode</li> <li>• Any Transport over MPLS: Ethernet over MPLS: VLAN ID Rewrite</li> <li>• Any Transport over MPLS: Frame Relay over MPLS</li> <li>• Any Transport over MPLS: AAL5 over MPLS</li> <li>• Any Transport over MPLS: ATM OAM Emulation</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|              | 12.2(33)SRA | AToM Tunnel Selection was introduced into this release on the Cisco 7600 router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|              | 12.2(33)SRB | <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB to support the following features on the Cisco 7600 router:</p> <ul style="list-style-type: none"> <li>• Any Transport over MPLS: Frame Relay over MPLS</li> <li>• Any Transport over MPLS: ATM Cell Relay over MPLS: Packed Cell Relay</li> <li>• Any Transport over MPLS: Ethernet over MPLS</li> <li>• <i>AToM Static Pseudowire Provisioning</i></li> </ul> <p>Platform-specific configuration information is contained in the following documents:</p> <ul style="list-style-type: none"> <li>• The “Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching” module of the <i>Cisco 7600 Series Cisco IOS Software Configuration Guide</i>, Release 12.2SR</li> <li>• The “Configuring Multiprotocol Label Switching on the Optical Services Modules” module of the <i>OSM Configuration Note</i>, Release 12.2SR</li> <li>• The “Configuring Multiprotocol Label Switching on FlexWAN and Enhanced FlexWAN Modules” module of the <i>FlexWAN and Enhanced FlexWAN Modules Configuration Guide</i></li> <li>• The “Configuring Any Transport over MPLS on a SIP” section of the <i>Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide</i></li> <li>• The “Configuring AToM VP Cell Mode Relay Support” section of the <i>Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide</i></li> <li>• The <i>Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers</i></li> </ul> |

Table 8 Feature Information for Any Transport over MPLS (continued)

| Feature Name | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.2(33)SXH | <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH and supports the following features:</p> <ul style="list-style-type: none"> <li>Any Transport over MPLS: Ethernet over MPLS: Port Mode</li> <li>Any Transport over MPLS: AAL5 over MPLS</li> <li>Any Transport over MPLS: ATM OAM Emulation</li> <li>Any Transport over MPLS: Single Cell Relay - VC Mode</li> <li>Any Transport over MPLS: ATM Cell Relay over MPLS - VP Mode</li> <li>Any Transport over MPLS: Packed Cell Relay - VC/VP Mode</li> <li>Any Transport over MPLS: Ethernet over MPLS</li> <li>ATM Port Mode Packed Cell Relay over AToM</li> <li>AToM Tunnel Selection</li> </ul> |
|              | 12.2(33)SRC | <p>The following feature was integrated into Cisco IOS Release 12.2(33)SRC:</p> <ul style="list-style-type: none"> <li>AToM Tunnel Selection support for the Cisco 7200 and Cisco 7300 routers was added.</li> <li>Per Subinterface MTU for Ethernet Over MPLS (EoMPLS)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.







## **MPLS Label Distribution Protocol**





# MPLS Label Distribution Protocol (LDP)

---

**First Published: January 1, 1999**

**Last Updated: May 1, 2008**

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network. This module explains the concepts related to MPLS LDP and describes how to configure MPLS LDP in a network.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS Label Distribution Protocol”](#) section on page 27.

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for MPLS LDP, page 2](#)
- [Information About MPLS LDP, page 2](#)
- [Information About MPLS LDP, page 2](#)
- [How to Configure MPLS LDP, page 5](#)
- [MPLS LDP Configuration Examples, page 20](#)
- [Command Reference, page 26](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

# Prerequisites for MPLS LDP

Label switching on a router requires that Cisco Express Forwarding (CEF) be enabled on that router.

## Information About MPLS LDP

To configure MPLS LDP, you should understand the following concepts:

- [Introduction to MPLS LDP, page 2](#)
- [MPLS LDP Functional Overview, page 2](#)
- [LDP and TDP Support, page 2](#)
- [Introduction to LDP Sessions, page 3](#)
- [Introduction to LDP Label Bindings, Label Spaces, and LDP Identifiers, page 4](#)

## Introduction to MPLS LDP

MPLS LDP provides the means for LSRs to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

MPLS LDP enables one LSR to inform another LSR of the label bindings it has made. Once a pair of routers communicate the LDP parameters, they establish a label-switched path (LSP). MPLS LDP enables LSRs to distribute labels along normally routed paths to support MPLS forwarding. This method of label distribution is also called hop-by-hop forwarding. With IP forwarding, when a packet arrives at a router the router looks at the destination address in the IP header, performs a route lookup, and forwards the packet to the next hop. With MPLS forwarding, when a packet arrives at a router the router looks at the incoming label, looks up the label in a table, and then forwards the packet to the next hop. MPLS LDP is useful for applications that require hop-by-hop forwarding, such as MPLS VPNs.

## MPLS LDP Functional Overview

Cisco MPLS LDP provides the building blocks for MPLS-enabled applications, such as MPS Virtual Private Networks (VPNs).

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

## LDP and TDP Support

LDP supersedes Tag Distribution Protocol (TDP). See [Table 1](#) for information about LDP and TDP support in Cisco IOS releases.

Use caution when upgrading the image on a router that uses TDP. Ensure that the TDP sessions are established when the new image is loaded. You can accomplish this by issuing the global configuration command **mpls label protocol tdp**. Issue this command and save it to the startup configuration before loading the new image. Alternatively, you can enter the command and save the running configuration immediately after loading the new image.

**Table 1**      **LDP and TDP Support**

| Train and Release        | LDP/TDP Support                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0S Train              | <ul style="list-style-type: none"> <li>• TDP is enabled by default.</li> <li>• Cisco IOS Release 12.0(29)S and earlier releases: TDP is supported for LDP features.</li> <li>• Cisco IOS Release 12.0(30)S and later releases: TDP is not support for LDP features.</li> </ul>                                                                                                                                                  |
| 12.2S, SB, and SR Trains | <ul style="list-style-type: none"> <li>• LDP is enabled by default.</li> <li>• Cisco IOS Release 12.2(25)S and earlier releases: TDP is supported for LDP features.</li> <li>• Cisco IOS Releases 12.2(27)SBA, 12.2(27)SRA, 12.2(27)SRB and later releases: TDP is not supported for LDP features.</li> </ul>                                                                                                                   |
| 12.T/Mainline Trains     | <ul style="list-style-type: none"> <li>• Cisco IOS Release 12.3(14)T and earlier releases: TDP is enabled by default.</li> <li>• Cisco IOS Releases 12.4 and 12.4T and later releases: LDP is enabled by default.</li> <li>• Cisco IOS Release 12.3(11)T and earlier releases: TDP is supported for LDP features.</li> <li>• Cisco IOS Release 12.3(14)T and later releases: TDP is not support ed for LDP features.</li> </ul> |

## Introduction to LDP Sessions

When you enable MPLS LDP, the LSRs send out messages to try to find other LSRs with which they can create LDP sessions. The following sections explain the differences between directly connected LDP sessions and nondirectly connected LDP sessions.

### Directly Connected MPLS LDP Sessions

If an LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends out LDP link Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet (multicast). A neighboring LSR may respond to the link Hello message, allowing the two routers to establish an LDP session. This is called basic discovery.

To initiate an LDP session between routers, the routers determine which router will take the active role and which router will take the passive role. The router that takes the active role establishes the LDP TCP connection session and initiates the negotiation of the LDP session parameters. To determine the roles, the two routers compare their transport addresses. The router with the higher IP address takes the active role and establishes the session.

After the LDP TCP connection session is established, the LSRs negotiate the session parameters, including the method of label distribution to be used. Two methods are available:

- Downstream Unsolicited: An LSR advertises label mappings to peers without being asked to.
- Downstream on Demand: An LSR advertises label mappings to a peer only when the peer asks for them.

For information about creating LDP sessions, see the [“Enabling Directly Connected LDP Sessions” section on page 6](#).

## Nondirectly Connected MPLS LDP Sessions

If the LSR is more than one hop from its neighbor, it is nondirectly connected to its neighbor. For these nondirectly connected neighbors, the LSR sends out a targeted Hello message as a UDP packet, but as a unicast message specifically addressed to that LSR. The nondirectly connected LSR responds to the Hello message and the two routers begin to establish an LDP session. This is called extended discovery.

An MPLS LDP targeted session is a label distribution session between routers that are not directly connected. When you create an MPLS traffic engineering tunnel interface, you need to establish a label distribution session between the tunnel headend and the tailend routers. You establish nondirectly connected MPLS LDP sessions by enabling the transmission of targeted Hello messages.

You can use the **mpls ldp neighbor targeted** command to set up a targeted session when other means of establishing targeted sessions do not apply, such as configuring **mpls ip** on a traffic engineering (TE) tunnel or configuring Any Transport over MPLS (AToM) virtual circuits (VCs). For example, you can use this command to create a targeted session between directly connected MPLS label switch routers (LSRs) when MPLS label forwarding convergence time is an issue.

The **mpls ldp neighbor targeted** command can improve label convergence time for directly connected neighbor LSRs when the link(s) directly connecting them are down. When the links between the neighbor LSRs are up, both the link and targeted Hellos maintain the LDP session. If the links between the neighbor LSRs go down, the targeted Hellos maintain the session, allowing the LSRs to retain labels learned from each other. When a link directly connecting the LSRs comes back up, the LSRs can immediately reinstall labels for forwarding use without having to reestablish their LDP session and exchange labels.

The exchange of targeted Hello messages between two nondirectly connected neighbors can occur in several ways, including the following:

- Router 1 sends targeted Hello messages carrying a response request to Router 2. Router 2 sends targeted Hello messages in response if its configuration permits. In this situation, Router 1 is considered to be *active* and Router 2 is considered to be *passive*.
- Router 1 and Router 2 both send targeted Hello messages to each other. Both routers are considered to be *active*. Both, one, or neither router can also be *passive*, if they have been configured to respond to requests for targeted Hello messages from each other.

The default behavior of an LSR is to ignore requests from other LSRs that send targeted Hello messages. You can configure an LSR to respond to requests for targeted Hello messages by issuing the **mpls ldp discovery targeted-hello accept** command.

The active LSR mandates the protocol that is used for a targeted session. The passive LSR uses the protocol of the received targeted Hello messages.

For information about creating MPLS LDP targeted sessions, see the [“Establishing Nondirectly Connected MPLS LDP Sessions”](#) section on page 8.

## Introduction to LDP Label Bindings, Label Spaces, and LDP Identifiers

An LDP label binding is an association between a destination prefix and a label. The label used in a label binding is allocated from a set of possible labels called a label space.

LDP supports two types of label spaces:

- **Interface-specific**—An interface-specific label space uses interface resources for labels. For example, label-controlled ATM (LC-ATM) interfaces use virtual path identifiers/virtual circuit identifiers (VPIs/VCI) for labels. Depending on its configuration, an LDP platform may support zero, one, or more interface-specific label spaces.

- Platform-wide—An LDP platform supports a single platform-wide label space for use by interfaces that can share the same labels. For Cisco platforms, all interface types, except LC-ATM, use the platform-wide label space.

LDP uses a 6-byte quantity called an LDP Identifier (or LDP ID) to name label spaces. The LDP ID is made up of the following components:

- The first four bytes, called the LDP router ID, identify the LSR that owns the label space.
- The last two bytes, called the local label space ID, identify the label space within the LSR. For the platform-wide label space, the last two bytes of the LDP ID are always both 0.

The LDP ID takes the following form:

<LDP router ID> : <local label space ID>

The following are examples of LDP IDs:

- 172.16.0.0:0
- 192.168.0.0:3

The router determines the LDP router ID as follows, if the **mpls ldp router-id** command is not executed,

1. The router examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

The normal (default) method for determining the LDP router ID may result in a router ID that is not usable in certain situations. For example, the router might select an IP address as the LDP router ID that the routing protocol cannot advertise to a neighboring router. The **mpls ldp router-id** command allows you to specify the IP address of an interface as the LDP router ID. Make sure the specified interface is operational so that its IP address can be used as the LDP router ID.

When you issue the **mpls ldp router-id** command without the **force** keyword, the router selects the IP address of the specified interface (provided that the interface is operational) the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is configured.

When you issue the **mpls ldp router-id** command with the **force** keyword, the effect of the **mpls ldp router-id** command depends on the current state of the specified interface:

- If the interface is up (operational) and if its IP address is not currently the LDP router ID, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down (not operational) when the **mpls ldp router-id force** command is issued, when the interface transitions to up, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

## How to Configure MPLS LDP

This section contains the following procedures:

- [Enabling Directly Connected LDP Sessions, page 6](#) (required)

- [Establishing Nondirectly Connected MPLS LDP Sessions, page 8](#) (optional)
- [Saving Configurations: MPLS/Tag Switching Commands, page 11](#) (optional)
- [Specifying the LDP Router ID, page 11](#) (optional)
- [Preserving QoS Settings with MPLS LDP Explicit Null, page 13](#) (optional)
- [Protecting Data Between LDP Peers with MD5 Authentication, page 17](#) (optional)

## Enabling Directly Connected LDP Sessions

This procedure explains how to configure MPLS LDP sessions between two directly connected routers.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mpls ip`
4. `mpls label protocol {ldp | tdp | both}`
5. `interface type number`
6. `mpls ip`
7. `exit`
8. `exit`
9. `show mpls interfaces [interface] [detail]`
10. `show mpls ldp discovery [all | vrf vpn-name] [detail]`
11. `show mpls ldp neighbor [[vrf vpn-name] [address | interface] [detail] | [all]]`

### DETAILED STEPS

|        | Command or Action                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                          |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <code>mpls ip</code><br><br><b>Example:</b><br>Router(config)# mpls ip               | Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>• The <code>mpls ip</code> command is enabled by default; you do not have to specify this command.</li> <li>• Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul> |

|         | Command or Action                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <pre>mpls label protocol {ldp   tdp   both}</pre> <p><b>Example:</b><br/>Router(config)# mpls label protocol ldp</p>                                | <p>Configures the use of LDP on all interfaces. LDP is the default.</p> <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul> |
| Step 5  | <pre>Router(config)# interface type number</pre> <p><b>Example:</b><br/>Router(config)# interface ethernet3/0</p>                                   | <p>Specifies the interface to be configured and enters interface configuration mode.</p>                                                                                                                                                                                                                               |
| Step 6  | <pre>mpls ip</pre> <p><b>Example:</b><br/>Router(config-if)# mpls ip</p>                                                                            | <p>Configures MPLS hop-by-hop forwarding on the interface.</p> <ul style="list-style-type: none"> <li>You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>                                                                                                                          |
| Step 7  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                                                  | <p>Exits interface configuration mode and enters global configuration mode.</p>                                                                                                                                                                                                                                        |
| Step 8  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config)# exit</p>                                                                                     | <p>Exits global configuration mode and enters privileged EXEC mode.</p>                                                                                                                                                                                                                                                |
| Step 9  | <pre>show mpls interfaces [interface] [detail]</pre> <p><b>Example:</b><br/>Router# show mpls interfaces</p>                                        | <p>Verifies that the interfaces have been configured to use LDP, TDP, or both.</p>                                                                                                                                                                                                                                     |
| Step 10 | <pre>show mpls ldp discovery [all   vrf vpn-name] [detail]</pre> <p><b>Example:</b><br/>Router# show mpls ldp discovery</p>                         | <p>Verifies that the interface is up and is sending Discovery Hello messages.</p>                                                                                                                                                                                                                                      |
| Step 11 | <pre>show mpls ldp neighbor [[vrf vpn-name] [address   interface] [detail]   [all]]</pre> <p><b>Example:</b><br/>Router# show mpls ldp neighbor</p> | <p>Displays the status of LDP sessions.</p>                                                                                                                                                                                                                                                                            |

## Examples

The following **show mpls interfaces** command verifies that interfaces Ethernet 1/0 and 1/1 have been configured to use LDP:

```
Router# show mpls interfaces
```

| Interface   | IP        | Tunnel | BGP | Static | Operational |
|-------------|-----------|--------|-----|--------|-------------|
| Ethernet3/0 | Yes (ldp) | No     | No  | No     | Yes         |
| Ethernet3/1 | Yes       | No     | No  | No     | Yes         |

The following **show mpls ldp discovery** command verifies that the interface is up and is sending LDP Discovery Hello messages (as opposed to TDP Hello messages):

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
 172.16.12.1:0
Discovery Sources:
Interfaces:
 Ethernet3/0 (ldp): xmit
```

The following example shows that the LDP session between routers was successfully established:

```
Router# show mpls ldp neighbor
```

```
Peer LDP Ident: 10.1.1.2:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.1.1.2.18 - 10.1.1.1.66
State: Oper; Msgs sent/rcvd: 12/11; Downstream
Up time: 00:00:10
LDP discovery sources:
FastEthernet1/0, Src IP addr: 10.20.10.2
Addresses bound to peer LDP Ident:
10.1.1.2 10.20.20.1 10.20.10.2
```

For examples on configuring directly connected LDP sessions, see the [“Configuring Directly Connected MPLS LDP Sessions: Example”](#) section on page 20.

## Establishing Nondirectly Connected MPLS LDP Sessions

This section explains how to configure nondirectly connected MPLS LDP sessions, which enable you to establish an LDP session between routers that are not directly connected.

### Prerequisites

- MPLS requires CEF.
- You must configure the routers at both ends of the tunnel to be active or enable one router to be passive with the **mpls ldp discovery targeted-hello accept** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol {ldp | tdp | both}**

5. **interface** *tunnelnumber*
6. **tunnel destination** *ip-address*
7. **mpls ip**
8. **exit**
9. **exit**
10. **show mpls ldp discovery** [*all* | *vrf vpn-name*] [*detail*]

## DETAILED STEPS

|        | Command or Action                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip                                                                       | Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>• The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>• Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul> |
| Step 4 | <b>mpls label protocol</b> { <i>ldp</i>   <i>tdp</i>   <i>both</i> }<br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp | Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>• If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>                                                     |
| Step 5 | <b>interface</b> <i>tunnelnumber</i><br><br><b>Example:</b><br>Router(config)# interface tunnell                                       | Configures a tunnel interface and enters interface configuration mode.                                                                                                                                                                                                                                                                                                |
| Step 6 | <b>tunnel destination</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-if)# tunnel destination<br>172.16.1.1              | Assigns an IP address to the tunnel interface.                                                                                                                                                                                                                                                                                                                        |
| Step 7 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                                                    | Configures MPLS hop-by-hop forwarding on the interface. <ul style="list-style-type: none"> <li>• You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>                                                                                                                                                                              |

|         | Command or Action                                                                                                                 | Purpose                                                                    |
|---------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                     | Exits interface configuration mode and enters global configuration mode.   |
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                        | Exits global configuration mode and enters privileged EXEC mode.           |
| Step 10 | <b>show mpls ldp discovery</b> [all   vrf <i>vpn-name</i> ]<br>[detail]<br><br><b>Example:</b><br>Router# show mpls ldp discovery | Verifies that the interface is up and is sending Discovery Hello messages. |

## Example

The following example shows the output of the **show mpls ldp discovery** command for a nondirectly connected LDP session.

```
Router# show mpls ldp discovery

Local LDP Identifier:
 172.16.0.0:0
Discovery Sources:
Interfaces:
 POS2/0 (ldp): xmit/recv
 LDP Id: 172.31.255.255:0
 Tunnell (ldp): Targeted -> 192.168.255.255
Targeted Hellos:
 172.16.0.0 -> 192.168.255.255 (ldp): active, xmit/recv
 LDP Id: 192.168.255.255:0
 172.16.0.0 -> 192.168.0.0 (tdp): passive, xmit/recv
 TDP Id: 192.168.0.0:0
```

This command output indicates that:

- The local LSR (172.16.0.0) sent LDP link Hello messages on interface POS2/0 and discovered neighbor 172.31.255.255.
- The local LSR sent LDP targeted Hello messages associated with interface Tunnell1 to target 192.168.255.255. The LSR was configured to use LDP.
- The local LSR is active for targeted discovery activity with 192.168.255.255; this means that the targeted Hello messages it sends to 192.168.255.255 carry a response request. The local LSR was configured to have an LDP session with the nondirectly connected LSR 192.168.255.255.
- The local LSR is not passive from the discovery activity with 192.168.255.255 for one of the following reasons:
  - The targeted Hello messages it receives from 192.168.255.255 do not carry a response request.
  - The local LSR has not been configured to respond to such requests.
- The local LSR sent TDP directed Hello messages to the target LSR 192.168.0.0. This LSR uses TDP because the Hello messages received from the target LSR 192.168.0.0 were TDP directed Hello messages.

- The local LSR is passive in discovery activity with LSR 192.168.0.0. This means that the directed Hello messages it receives from LSR 192.168.0.0 carry a response request and that the local LSR has been configured with the **mpls ldp discovery targeted-hello accept** command to respond to such requests from LSR 192.168.0.0.
- The local LSR is not active in discovery activity with LSR 192.168.0.0, because no application that requires an LDP session with LSR 192.168.0.0 has been configured on the local LSR.

For examples of configuring LDP targeted sessions, see the “[Establishing Nondirectly Connected MPLS LDP Sessions: Example](#)” section on page 22.

## Saving Configurations: MPLS/Tag Switching Commands

In releases of Cisco IOS software prior to 12.4(2)T, some MPLS commands had both a tag-switching version and an MPLS version. For example, the two commands **tag-switching ip** and **mpls ip** were the same. To support backward compatibility, the tag-switching form of the command was written to the saved configuration.

Starting in Cisco IOS Release 12.4(2)T, the MPLS form of the command is written to the saved configuration.

For example, if an ATM interface is configured using the following commands, which have both a tag-switching form and an MPLS form:

```
Router(config)# interface ATM3/0
Router(config-if)# ip unnumbered Loopback0
router(config-if)# tag-switching ip
Router(config-if)# mpls label protocol ldp
```

After you enter these commands and save this configuration or display the running configuration with the **show running** command, the commands saved or displayed appear as follows:

```
interface ATM3/0
ip unnumbered Loopback0
mpls ip
mpls label protocol ldp
```

## Specifying the LDP Router ID

The **mpls ldp router-id** command allows you to establish the IP address of an interface as the LDP router ID.

The following steps describe the normal process for determining the LDP router ID:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

- If the loopback interface has been explicitly shut down.
- If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, make sure that the routing protocol in use is configured to advertise the corresponding /32 network.

- Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router.

The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the command is delayed until the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

## Prerequisites

Make sure the specified interface is operational before assigning it as the LDP router ID.

## SUMMARY STEPS

- enable**
- configure terminal**
- mpls ip**
- mpls label protocol {ldp | tdp | both}**
- mpls ldp router-id interface [force]**
- exit**
- show mpls ldp discovery [all | detail |vrf vpn-name]**

## DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                                 |
|--------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                       |

|        | Command or Action                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip                                                       | Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul> |
| Step 4 | <b>mpls label protocol {ldp   tdp   both}</b><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp        | Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>                                                   |
| Step 5 | <b>mpls ldp router-id interface [force]</b><br><br><b>Example:</b><br>Router(config)# mpls ldp router-id pos2/0/0      | Specifies the preferred interface for determining the LDP router ID.                                                                                                                                                                                                                                                                                              |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                             | Exits global configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                  |
| Step 7 | <b>show mpls ldp discovery [all   detail   vrf vpn-name]</b><br><br><b>Example:</b><br>Router# show mpls ldp discovery | Displays the LDP identifier for the local router.                                                                                                                                                                                                                                                                                                                 |

## Example

The following example assigns interface pos2/0/0 as the LDP router ID:

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp router-id pos2/0/0 force
```

The following example displays the LDP router ID (10.15.15.15):

```
Router# show mpls ldp discovery

Local LDP Identifier:
 10.15.15.15:0
Discovery Sources:
 Interfaces:
 Ethernet4 (ldp): xmit/rcv
 LDP Id: 10.14.14.14:0
```

## Preserving QoS Settings with MPLS LDP Explicit Null

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the second last (penultimate) label switched router (LSR) to remove the MPLS header from the packet. In this case, the penultimate LSR and the last LSR do not have access to the quality of service (QoS) values that the packet carried before the MPLS header was removed. To preserve the QoS values, you can configure the LSR to advertise an explicit NULL label (a label value of zero). The LSR at the penultimate hop forwards MPLS packets with a NULL label instead of forwarding IP packets.

**Note**

An explicit NULL label is not needed when the penultimate hop receives MPLS packets with a label stack that contains at least two labels and penultimate hop popping is performed. In that case, the inner label can still carry the QoS value needed by the penultimate and edge LSR to implement their QoS policy.

When you issue the **mpls ldp explicit-null** command, Explicit Null is advertised in place of Implicit Null for directly connected prefixes.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol {ldp | tdp | both}**
5. **interface** *type number*
6. **mpls ip**
7. **exit**
8. **mpls ldp explicit-null** [**for** *prefix-acl* | **to** *peer-acl* | **for** *prefix-acl to peer-acl*]
9. **exit**
10. **show mpls forwarding-table** [*network {mask | length}* | **labels** *label* [- *label*] | **interface** *interface* | *next-hop address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vpn-name*] [**detail**]

**DETAILED STEPS**

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|         | Command or Action                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                           |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3  | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip                                                                                                                                                                            | Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul> |
| Step 4  | <b>mpls label protocol {ldp   tdp   both}</b><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp                                                                                                                             | Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>                                                   |
| Step 5  | <b>interface type number</b><br><br><b>Example:</b><br>Router(config)# interface atm2/0                                                                                                                                                     | Specifies the interface to be configured and enters interface configuration mode.                                                                                                                                                                                                                                                                                 |
| Step 6  | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                                                                                                                                                         | Configures MPLS hop-by-hop forwarding on the interface. <ul style="list-style-type: none"> <li>You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>                                                                                                                                                                            |
| Step 7  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                                                               | Exits interface configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                                          |
| Step 8  | <b>mpls ldp explicit-null [for prefix-acl   to peer-acl   for prefix-acl to peer-acl]</b><br><br><b>Example:</b><br>Router(config)# mpls ldp explicit-null                                                                                  | Advertises an Explicit Null label in situations where it would normally advertise an Implicit Null label.                                                                                                                                                                                                                                                         |
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                                                  | Exits global configuration mode and enter privileged EXEC mode.                                                                                                                                                                                                                                                                                                   |
| Step 10 | <b>show mpls forwarding-table [network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]] [vrf vpn-name] [detail]</b><br><br><b>Example:</b><br>Router# show mpls forwarding-table | Verifies that MPLS packets are forwarded with an explicit-null label (value of 0).                                                                                                                                                                                                                                                                                |

## Examples

Enabling explicit-null on an egress LSR causes that LSR to advertise the explicit-null label to all adjacent MPLS routers.

```
Router# configure terminal
```

```
Router(config)# mpls ldp explicit-null
```

If you issue the **show mpls forwarding-table** command on an adjacent router, the output shows that MPLS packets are forwarded with an explicit-null label (value of 0). In the following example, the second column shows that entries have outgoing labels of 0, where once they were marked “Pop label”.

```
Router# show mpls forwarding-table
```

| Local label | Outgoing label or VC | Prefix or Tunnel Id | Bytes switched | label | Outgoing interface | Next Hop     |
|-------------|----------------------|---------------------|----------------|-------|--------------------|--------------|
| 19          | Pop tag              | 10.12.12.12/32      | 0              |       | Fa2/1/0            | 172.16.0.1   |
| 22          | 0                    | 10.14.14.14/32      | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 23          | 0                    | 172.24.24.24/32     | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 24          | 0                    | 192.168.0.0/8       | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 25          | 0                    | 10.15.15.15/32      | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 26          | 0                    | 172.16.0.0/8        | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 27          | 25                   | 10.16.16.16/32      | 0              |       | Fa2/0/0            | 192.168.0.22 |
| 28          | 0                    | 10.34.34.34/32      | 0              |       | Fa2/0/0            | 192.168.0.2  |

Enabling explicit-null and specifying the **for** keyword with a standard access control list (ACL) changes all adjacent MPLS routers' tables to swap an explicit-null label for only those entries specified in the access-list. In the following example, an access-list is created that contains the 10.24.24.24/32 entry. Explicit null is configured and the access list is specified.

```
Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# access-list 24 permit host 10.24.24.24
Router(config)# mpls ldp explicit-null for 24
```

If you issue the **show mpls forwarding-table** command on an adjacent router, the output shows that the only the outgoing labels for the addresses specified (172.24.24.24/32) change from Pop label to 0. All other Pop label outgoing labels remain the same.

```
Router# show mpls forwarding-table
```

| Local label | Outgoing label or VC | Prefix or Tunnel Id | Bytes switched | label | Outgoing interface | Next Hop     |
|-------------|----------------------|---------------------|----------------|-------|--------------------|--------------|
| 19          | Pop tag              | 10.12.12.12/32      | 0              |       | Fa2/1/0            | 172.16.0.1   |
| 22          | 0                    | 10.14.14.14/32      | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 23          | 0                    | 172.24.24.24/32     | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 24          | 0                    | 192.168.0.0/8       | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 25          | 0                    | 10.15.15.15/32      | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 26          | 0                    | 172.16.0.0/8        | 0              |       | Fa2/0/0            | 192.168.0.2  |
| 27          | 25                   | 10.16.16.16/32      | 0              |       | Fa2/0/0            | 192.168.0.22 |
| 28          | 0                    | 10.34.34.34/32      | 0              |       | Fa2/0/0            | 192.168.0.2  |

Enabling explicit null and adding the **to** keyword and an access list enables you to advertise explicit-null labels to only those adjacent routers specified in the access-list. To advertise explicit-null to a particular router, you must specify the router's LDP ID in the access-list.

In the following example, an access-list contains the 10.15.15.15/32 entry, which is the LDP ID of an adjacent MPLS router. The router that is configured with explicit null advertises explicit-null labels only to that adjacent router.

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
 10.15.15.15:0
Discovery Sources:
 Interfaces:
 Ethernet4 (ldp): xmit/recv
 TDP Id: 10.14.14.14:0
```

```

Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# access-list 15 permit host 10.15.15.15
Router(config)# mpls ldp explicit-null to 15

```

If you issue the **show mpls forwarding-table** command, the output shows that explicit null labels are going only to the router specified in the access list.

```
Router# show mpls forwarding-table
```

| Local label | Outgoing label or VC tag | Prefix or Tunnel Id | Bytes label switched | Outgoing interface | Next Hop     |
|-------------|--------------------------|---------------------|----------------------|--------------------|--------------|
| 19          | Pop tag                  | 10.12.12.12/32      | 0                    | Fa2/1/0            | 172.16.0.1   |
| 22          | 0                        | 10.14.14.14/32      | 0                    | Fa2/0/0            | 192.168.0.2  |
| 23          | 0                        | 172.24.24.24/32     | 0                    | Fa2/0/0            | 192.168.0.2  |
| 24          | 0                        | 192.168.0.0/8       | 0                    | Fa2/0/0            | 192.168.0.2  |
| 25          | 0                        | 10.15.15.15/32      | 0                    | Fa2/0/0            | 192.168.0.2  |
| 26          | 0                        | 172.16.0.0/8        | 0                    | Fa2/0/0            | 192.168.0.2  |
| 27          | 25                       | 10.16.16.16/32      | 0                    | Fa2/0/0            | 192.168.0.22 |
| 28          | 0                        | 10.34.34.34/32      | 0                    | Fa2/0/0            | 192.168.0.2  |

Enabling explicit-null with both the **for** and **to** keywords enables you to specify which routes to advertise with explicit-null labels and to which adjacent routers to advertise these explicit-null labels.

```
Router# show access 15
```

```

Standard IP access list 15
 permit 10.15.15.15 (7 matches)

```

```
Router# show access 24
```

```

Standard IP access list 24
 permit 10.24.24.24 (11 matches)

```

```

Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp explicit-null for 24 to 15

```

If you issue the **show mpls forwarding-table** command on the router called 47K-60-4, the output shows that it receives explicit null labels for 10.24.24.24/32.

```
Router# show mpls forwarding-table
```

| Local label | Outgoing label or VC | Prefix or Tunnel Id | Bytes label switched | Outgoing interface | Next Hop   |
|-------------|----------------------|---------------------|----------------------|--------------------|------------|
| 17          | 0 <---               | 10.24.24.24/32      | 0                    | Et4                | 172.16.0.1 |
| 20          | Pop tag              | 172.16.0.0/8        | 0                    | Et4                | 172.16.0.1 |
| 21          | 20                   | 10.12.12.12/32      | 0                    | Et4                | 172.16.0.1 |
| 22          | 16                   | 10.0.0.0/8          | 0                    | Et4                | 172.16.0.1 |
| 23          | 21                   | 10.13.13.13/32      | 0                    | Et4                | 172.16.0.1 |
| 25          | Pop tag              | 10.14.14.14/32      | 0                    | Et4                | 172.16.0.1 |
| 27          | Pop tag              | 192.168.0.0/8       | 0                    | Et4                | 172.16.0.1 |
| 28          | 25                   | 10.16.16.16/32      | 0                    | Et4                | 172.16.0.1 |
| 29          | Pop tag              | 192.168.34.34/32    | 0                    | Et4                | 172.16.0.1 |

## Protecting Data Between LDP Peers with MD5 Authentication

You can enable authentication between two LDP peers, which verifies each segment sent on the TCP connection between the peers. You must configure authentication on both LDP peers using the same password; otherwise, the peer session is not established.

Authentication uses the Message Digest 5 (MD5) algorithm to verify the integrity of the communication and authenticate the origin of the message.

To enable authentication, issue the **mpls ldp neighbor** command with the **password** keyword. This causes the router to generate an MD5 digest for every segment sent on the TCP connection and check the MD5 digest for every segment received from the TCP connection.

When you configure a password for an LDP neighbor, the router tears down existing LDP sessions and establishes new sessions with the neighbor.

If a router has a password configured for a neighbor, but the neighboring router does not have a password configured, a message such as the following appears on the console who has a password configured while the two routers attempt to establish an LDP session. The LDP session is not established.

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address](11003) to [local router's IP address] (646)
```

Similarly, if the two routers have different passwords configured, a message such as the following appears on the console. The LDP session is not established.

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address](11004) to [local router's IP address] (646)
```

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol {ldp | tdp | both}**
5. **mpls ldp neighbor [vrf vpn-name] ip-address [password [0-7] password-string]**
6. **show mpls ldp neighbor [[vrf vpn-name] [address | interface] [detail] | [all]]**

## DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|        | Command or Action                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip                                                                                                                | Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul> |
| Step 4 | <b>mpls label protocol {ldp   tdp   both}</b><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp                                                                 | Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>                                                   |
| Step 5 | <b>mpls ldp neighbor [vrf vpn-name] ip-address [password [0-7] password-string]</b><br><br><b>Example:</b><br>Router(config)# mpls ldp neighbor 172.27.0.15 password onethirty9 | Specifies authentication between two LDP peers.                                                                                                                                                                                                                                                                                                                   |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                      | Exits global configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                  |
| Step 7 | <b>show mpls ldp neighbor [[vrf vpn-name] [address   interface] [detail]   [all]]</b><br><br><b>Example:</b><br>Router# show mpls ldp neighbor detail                           | Displays the status of LDP sessions.<br><br>If the passwords have been set on both LDP peers and the passwords match, the <b>show mpls ldp neighbor</b> command displays that the LDP session was successfully established.                                                                                                                                       |

## Examples

The following example configures a router with the password cisco:

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp neighbor 10.1.1.1 password cisco
Router(config)# exit
```

The following example shows that the LDP session between routers was successfully established:

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.1.1.2:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.1.1.2.11118 - 10.1.1.1.646
State: Oper; Msgs sent/rcvd: 12/11; Downstream
Up time: 00:00:10
LDP discovery sources:
FastEthernet1/0, Src IP addr: 10.20.10.2
Addresses bound to peer LDP Ident:
10.1.1.2 10.20.20.1 10.20.10.2
```

The following **show mpls ldp neighbor detail** command shows that MD5 (shown in bold) is used for the LDP session.

```
Router# show mpls ldp neighbor 10.0.0.21 detail

Peer LDP Ident: 10.0.0.21:0; Local LDP Ident 10.0.0.22:0
TCP connection: 10.0.0.21.646 - 10.0.0.22.14709; MD5 on
State: Oper; Msgs sent/rcvd: 1020/1019; Downstream; Last TIB rev sent 2034
Up time: 00:00:39; UID: 3; Peer Id 1;
LDP discovery sources:
 FastEthernet1/1; Src IP addr: 172.16.1.1
 holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
 10.0.0.21 10.0.38.28 10.88.88.2 172.16.0.1
 172.16.1.1
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

## MPLS LDP Configuration Examples

This section includes the following configuration examples:

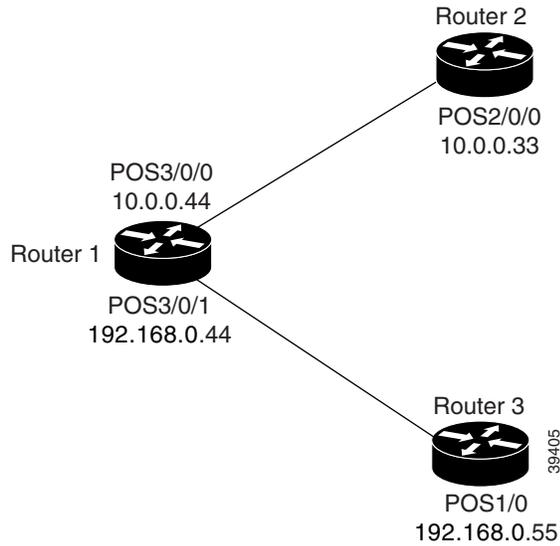
- [Configuring Directly Connected MPLS LDP Sessions: Example, page 20](#)
- [Establishing Nondirectly Connected MPLS LDP Sessions: Example, page 22](#)

### Configuring Directly Connected MPLS LDP Sessions: Example

[Figure 1](#) shows a sample network for configuring directly connected LDP sessions.

This example configures the following:

- MPLS hop-by-hop forwarding for the POS links between Router 1 and Router 2 and between Router 1 and Router 3.
- LDP for label distribution between Router 1 and Router 2.
- TDP for label distribution between Router 1 and Router 3.
- A loopback interface and IP address for each LSR that can be used as the LDP router ID.

**Figure 1** Configuration of MPLS LDP**Note**

The configuration examples below show only the commands related to configuring LDP for Router 1, Router 2, and Router 3 in the sample network shown in [Figure 1](#).

**Router 1 Configuration**

```

ip cef distributed
interface Loopback0
ip address 172.16.0.11 255.255.255.255
!
interface POS3/0/0
ip address 10.0.0.44 255.0.0.0
mpls ip
mpls label protocol ldp
!
interface POS3/0/1
ip address 192.168.0.44 255.0.0.0
mpls ip
mpls label protocol tdp

```

!Assumes R1 supports distributed CEF  
!Loopback interface for LDP ID.

!Enable hop-by-hop MPLS forwarding  
!Use LDP for this interface

!Enable hop-by-hop MPLS forwarding  
!Use TDP for this interface

**Router 2 Configuration**

```

ip cef distributed
!
interface Loopback0
ip address 172.16.0.22 255.255.255.255
!
interface POS2/0/0
ip address 10.0.0.33 255.0.0.0
mpls ip
mpls label protocol ldp

```

!Assumes R2 supports distributed CEF  
!Loopback interface for LDP ID.

!Enable hop-by-hop MPLS forwarding  
!Use LDP for this interface

**Router 3 Configuration**

```

ip cef
!
interface Loopback0
ip address 172.16.0.33 255.255.255.255
!

```

!Assumes R3 does not support dCEF  
!Loopback interface for LDP ID.

```

interface POS1/0
ip address 192.168.0.55 255.0.0.0
mpls ip !Enable hop-by-hop MPLS forwarding
mpls label protocol tdp !Use TDP for this interface

```

The LDP configuration for Router 1 uses the **mpls label protocol ldp** command in interface configuration mode, because some of its interfaces use LDP and some use TDP. Another way to configure Router 1 is to use the **mpls label protocol ldp** command in global configuration mode to configure LDP as the default protocol for interfaces and use the **mpls label protocol tdp** command in interface configuration mode to configure TDP for the POS3/0/1 link to Router 3. This alternative way to configure Router 1 is shown below:

### Router 1 Configuration

```

ip cef distributed !Assumes R1 supports dCEF
mpls label protocol ldp !Use LDP for the default protocol
!
interface Loopback0 !Loopback interface for LDP ID.
ip address 172.16.0.11 255.255.255.255
interface POS3/0/0
ip address 10.0.0.44 255.0.0.0
mpls ip !Enable hop-by-hop MPLS forwarding
 !Use LDP (configured i/f default)

interface POS3/0/1
ip address 192.168.0.44 255.0.0.0
mpls ip !Enable hop-by-hop MPLS forwarding
mpls label protocol tdp !Use TDP for this interface

```

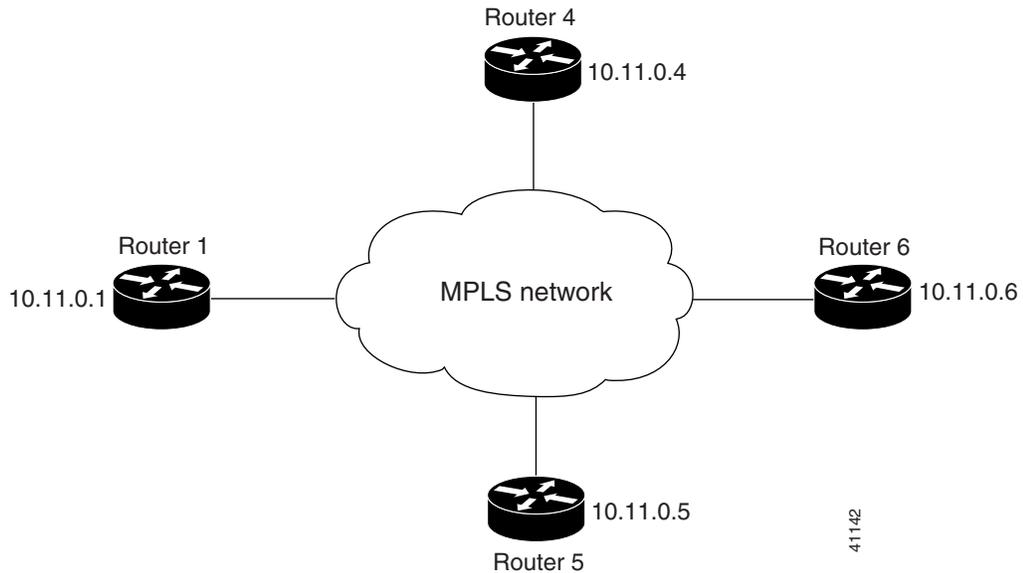
The configuration of Router 2 also uses the **mpls label protocol ldp** command in interface configuration mode. To specify LDP for all interfaces, use the **mpls label protocol ldp** command in global configuration mode without any interface **mpls label protocol** commands.

Configuring the **mpls ip** command on an interface triggers the transmission of discovery Hello messages for the interface.

## Establishing Nondirectly Connected MPLS LDP Sessions: Example

The following examples illustrate the configuration of platforms for MPLS LDP nondirectly connected sessions using the sample network shown in [Figure 2](#). Note that Routers 1, 4, 5, and 6 in this sample network are not directly connected to each other.

**Figure 2** Sample Network for Configuring LDP for Targeted Sessions



The configuration example shows the following:

- Targeted sessions between Routers 1 and 4 use LDP. Routers 1 and 4 are both active.
- Targeted sessions between Routers 1 and 6 use LDP. Router 1 is active and Router 6 is passive.
- Targeted sessions between Routers 1 and 5 use TDP. Router 5 is active.

These examples assume that the active ends of the nondirectly connected sessions are associated with tunnel interfaces, such as MPLS traffic engineering tunnels. They show only the commands related to configuring LDP targeted sessions. The examples do not show configuration of the applications that initiate the targeted sessions.

### Router 1 Configuration

Tunnel interfaces Tunnel14 and Tunnel16 specify LDP for targeted sessions associated with these interfaces. The targeted session for Router 5 requires TDP. The **mpls label protocol ldp** command in global configuration mode makes it unnecessary to explicitly specify LDP as part of the configuration from the Tunnel14 and Tunnel16.

```
ip cef distributed !Router1 supports distributed CEF

mpls label protocol ldp !Use LDP as default for all interfaces

interface Loopback0 !Loopback interface for LDP ID.
ip address 10.25.0.11 255.255.255.255

interface Tunnel14 !Tunnel to Router 4 requiring label distribution
tunnel destination 10.11.0.4 !Tunnel endpoint is Router 4
mpls ip !Enable hop-by-hop forwarding on the interface

interface Tunnel15 !Tunnel to Router 5 requiring label distribution
tunnel destination 10.11.0.5 !Tunnel endpoint is Router 5
mpls label protocol tdp !Use TDP for session with Router 5
mpls ip !Enable hop-by-hop forwarding on the interface

interface Tunnel16 !Tunnel to Router 6 requiring label distribution
tunnel destination 10.11.0.6 !Tunnel endpoint is Router 6
```

```
mpls ip !Enable hop-by-hop forwarding on the interface
```

#### Router 4 Configuration

The **mpls label protocol ldp** command in global configuration mode makes it unnecessary to explicitly specify LDP as part of the configuration for the Tunnel41 targeted session with Router 1.

```
ip cef distributed !Router 4 supports distributed CEF

mpls label protocol ldp !Use LDP as default for all interfaces

interface Loopback0 !Loopback interface for LDP ID.
ip address 10.25.0.44 255.255.255.255

interface Tunnel41 !Tunnel to Router 1 requiring label distribution
tunnel destination 10.11.0.1 !Tunnel endpoint is Router 1
mpls ip !Enable hop-by-hop forwarding on the interface
```

#### Router 5 Configuration

Router 5 must use TDP for all targeted sessions. Therefore, its configuration includes the **mpls label protocol tdp** command.

```
ip cef !Router 5 supports CEF

mpls label protocol tdp !Use TDP as default for all interfaces

interface Loopback0 !Loopback interface for LDP ID.
ip address 10.25.0.55 255.255.255.255

interface Tunnel51 !Tunnel to Router 1 requiring label distribution
tunnel destination 10.11.0.1 !Tunnel endpoint is Router 1
mpls ip !Enable hop-by-hop forwarding on the interface
```

#### Router 6 Configuration

By default, a router cannot be a passive neighbor in targeted sessions. Therefore, Router 1, Router 4, and Router 5 are active neighbors in any targeted sessions. The **mpls ldp discovery targeted-hello accept** command permits Router 6 to be a passive target in targeted sessions with Router 1. Router 6 can also be an active neighbor in targeted sessions, although the example does not include such a configuration.

```
ip cef distributed !Router 6 supports distributed CEF

interface Loopback0 !Loopback interface for LDP ID.
ip address 10.25.0.66 255.255.255.255

mpls ldp discovery targeted-hellos accept from LDP_SOURCES
 !Respond to requests for targeted hellos
 !from sources permitted by acl LDP_SOURCES

ip access-list standard LDP_SOURCES !Define acl for targeted hello sources.
permit 10.11.0.1 !Accept targeted hello request from Router 1.
deny any !Deny requests from other sources.
```

## Additional References

The following sections provide references related to MPLS LDP.

## Related Documents

| Related Topic                                                                                 | Document Title                                                         |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Configures LDP on every interface associated with a specified IGP instance.                   | <a href="#">MPLS LDP Autoconfiguration</a>                             |
| Ensures that LDP is fully established before the IGP path is used for switching.              | <a href="#">MPLS LDP-IGP Synchronization</a>                           |
| Allows ACLs to control the label bindings that an LSR accepts from its peer LSRs.             | <a href="#">MPLS LDP Inbound Label Binding Filtering</a>               |
| Enables standard, SNMP-based network management of the label switching features in Cisco IOS. | <a href="#">MPLS Label Distribution Protocol MIB Version 8 Upgrade</a> |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB                                                                                                                                                                                                       | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>MPLS Label Distribution Protocol MIB (draft-ietf-mpls-ldp-mib-08.txt)</li> <li>SNMP-VACM-MIB<br/>The View-based Access Control Model (ACM) MIB for SNMP</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title                    |
|----------|--------------------------|
| RFC 3036 | <i>LDP Specification</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mo/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mo/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.:

- **mpls label protocol** (global configuration)
- **mpls ldp router-id**

# Feature Information for MPLS Label Distribution Protocol

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS Label Distribution Protocol Overview

| Feature Name                     | Releases                                                                                                                                                         | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Label Distribution Protocol | 12.0(10)ST<br>12.0(14)ST<br>12.1(2)T<br>12.1(8a)E<br>12.2(2)T<br>12.2(4)T<br>12.2(8)T<br>12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.4(3)<br>12.4(5) | <p>This feature was introduced in Cisco IOS Release 12.0(10)ST, incorporating a new set of Multiprotocol Label Switching (MPLS) CLI commands implemented for use with Cisco routers and switches. The CLI commands in this release reflected MPLS command syntax and terminology, thus facilitating the orderly transition from a network using the Tag Distribution Protocol (TDP) to one using the Label Distribution Protocol (LDP).</p> <p>In Cisco IOS Release 12.0(14)ST, several new MPLS CLI commands were introduced, support for MPLS VPNs was added by means of a new <i>vrf vpn-name</i> parameter in certain existing commands, and other commands were modified to ensure consistent interpretation of associated <i>prefix-access-list</i> arguments by Cisco IOS software.</p> <p>In Cisco IOS 12.1(2)T, this feature was integrated into this release. Also, the <b>debug mpls atm-ldp api</b>, <b>debug mpls atm-ldp routes</b>, and <b>debug mpls atm-ldp states</b> commands were modified.</p> <p>This feature was integrated into Cisco IOS Release 12.1(8a)E.</p> <p>This feature was integrated into Cisco IOS Release 12.2(2)T.</p> |

Table 2 Feature Information for MPLS Label Distribution Protocol Overview (continued)

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <p>In Cisco IOS Release 12.2(4)T, support was added for Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR card, and the VPI range in the <b>show mpls atm-ldp bindings</b> and <b>show mpls ip binding</b> commands was changed to 4095.</p> <p>In Cisco IOS Release 12.2(8)T, the <b>debug mpls atm-ldp failure</b> command was introduced.</p> <p>In Cisco IOS Release 12.0(21)ST, the <b>mpls ldp neighbor implicit-withdraw</b> command was introduced.</p> <p>This feature was integrated into Cisco IOS Release 12.0(22)S. The <b>mpls ldp neighbor targeted-session</b> command and the <b>interface</b> keyword for the <b>mpls ldp advertise-labels</b> command were added.</p> <p>This feature was integrated into Cisco IOS Release 12.0(23)S. Default values for the <b>mpls ldp discovery</b> command <b>holdtime</b> and <b>interval</b> keywords were changed.</p> <p>This feature was integrated into Cisco IOS Release 12.2(13)T.</p> <p>In Cisco IOS Release 12.4(3), the default MPLS label distribution protocol changed from TDP to LDP. See <a href="#">“LDP and TDP Support” section on page 2</a> for more information. If no protocol is explicitly configured by the <b>mpls label protocol</b> command, LDP is the default label distribution protocol. See the <b>mpls label protocol</b> (global configuration) command for more information.</p> <p>Also in Cisco IOS Release 12.4(3), LDP configuration commands are saved by using the MPLS form of the command rather than the tag-switching form. Previously, commands were saved by using the tag-switching form of the command, for backward compatibility. See the <a href="#">“Saving Configurations: MPLS/Tag Switching Commands” section on page 11</a> for more information.</p> <p>In Cisco IOS Release 12.4(5), the <b>vrf vrf-name</b> keyword/argument pair was added for the <b>mpls ldp router-id</b> command to allow you to associate the LDP router ID with a nondefault VRF.</p> |

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, 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. (0801R)

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.

© 1999-2008 Cisco Systems, Inc. All rights reserved.



# MPLS LDP Session Protection

---

**First Published: November 8, 2004**

**Last Updated: May 31, 2007**

The MPLS LDP Session Protection feature provides faster label distribution protocol convergence when a link recovers following an outage. MPLS LDP Session Protection protects a label distribution protocol (LDP) session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel.

## **Finding Feature Information in This Module**

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS LDP Session Protection](#)” section on page 23.*

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Information About MPLS LDP Session Protection, page 2](#)
- [How to Configure MPLS LDP Session Protection, page 2](#)
- [Configuration Examples for MPLS LDP Session Protection, page 7](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)
- [Feature Information for MPLS LDP Session Protection, page 23](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Information About MPLS LDP Session Protection

MPLS LDP Session Protection maintains LDP bindings when a link fails. MPLS LDP sessions are protected through the use of LDP Hello messages. When you enable MPLS LDP, the label switched routers (LSRs) send messages to find other LSRs with which they can create LDP sessions.

- If the LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends out LDP Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet. The hello message is called an LDP Link Hello. A neighboring LSR responds to the hello message and the two routers begin to establish an LDP session.
- If the LSR is more than one hop from its neighbor, it is not directly connected to its neighbor. The LSR sends out a directed hello message as a UDP packet, but as a unicast message specifically addressed to that LSR. The hello message is called an LDP Targeted Hello. The nondirectly connected LSR responds to the Hello message and the two routers establish an LDP session. (If the path between two LSRs has been traffic engineered and has LDP enabled, the LDP session between them is called a targeted session.)

MPLS LDP Session Protection uses LDP Targeted Hellos to protect LDP sessions. Take, for example, two directly connected routers that have LDP enabled and can reach each other through alternate IP routes in the network. An LDP session that exists between two routers is called an LDP Link Hello Adjacency. When MPLS LDP Session Protection is enabled, an LDP Targeted Hello Adjacency is also established for the LDP session. If the link between the two routers fails, the LDP Link Adjacency also fails. However, if the LDP peer is still reachable through IP, the LDP session stays up, because the LDP Targeted Hello Adjacency still exists between the routers. When the directly connected link recovers, the session does not need to be reestablished, and LDP bindings for prefixes do not need to be relearned.

## How to Configure MPLS LDP Session Protection

This section explains how to configure and verify MPLS LDP Session Protection:

- [Enabling MPLS LDP Session Protection, page 2](#) (required)
- [Customizing MPLS LDP Session Protection, page 5](#) (optional)
- [Verifying MPLS LDP Session Protection, page 6](#) (optional)

## Enabling MPLS LDP Session Protection

You use the **mpls ldp session protection** command to enable MPLS LDP Session Protection. This command enables LDP sessions to be protected during a link failure. By default, the command protects all LDP sessions. The command has several options that enable you to specify which LDP sessions to protect. The **vrf** keyword lets you protect LDP sessions for a specified VRF. The **for** keyword lets you specify a standard IP access control list (ACL) of prefixes that should be protected. The **duration** keyword enables you to specify how long the router should retain the LDP Targeted Hello Adjacency following the loss of the LDP Link Hello Adjacency.

## Prerequisites

LSRs must be able to respond to LDP targeted hellos. Otherwise, the LSRs cannot establish a targeted adjacency. All routers that participate in MPLS LDP Session Protection must be enabled to respond to targeted hellos. Both neighbor routers must be configured for session protection or one router must be configured for session protection and the other router must be configured to respond to targeted hellos.

## Restrictions

This feature is not supported under the following circumstances:

- With TDP sessions
- With extended access lists
- With LC-ATM routers

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [distributed]
4. **interface loopback***number*
5. **ip address** {*prefix mask*}
6. **interface** *interface*
7. **mpls ip**
8. **mpls label protocol** {**ldp** | **tdp** | **both**}
9. **exit**
10. **mpls ldp session protection** [**vrf** *vpn-name*] [**for** *acl*] [**duration** *seconds*]

## DETAILED STEPS

|        | Command or Action                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>ip cef [distributed]</b><br><br><b>Example:</b><br>Router(config)# ip cef                                          | Configures Cisco Express Forwarding.                                                                                                                                                                                                                                                                                                                                |
| Step 4 | <b>interface loopbacknumber</b><br><br><b>Example:</b><br>Router(config)# interface Loopback0                         | Configures a loopback interface and enters interface configuration mode.                                                                                                                                                                                                                                                                                            |
| Step 5 | <b>ip address {prefix mask}</b><br><br><b>Example:</b><br>Router(config-if)# ip address 10.25.0.11<br>255.255.255.255 | Assigns an IP address to the loopback interface.                                                                                                                                                                                                                                                                                                                    |
| Step 6 | <b>interface interface</b><br><br><b>Example:</b><br>Router(config-if)# interface POS3/0                              | Specifies the interface to configure.                                                                                                                                                                                                                                                                                                                               |
| Step 7 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                                   | Configures MPLS hop-by-hop forwarding for a specified interface.                                                                                                                                                                                                                                                                                                    |
| Step 8 | <b>mpls label protocol {ldp   tdp   both}</b><br><br><b>Example:</b><br>Router(config-if)# mpls label protocol ldp    | Configures the use of LDP on a specific interface or on all interfaces.<br><br>In interface configuration mode, the command sets the default label distribution protocol for the interface to be LDP, overriding any default set by the global <b>mpls label protocol</b> command.<br><br>In global configuration mode, the command sets all the interfaces to LDP. |

|         | Command or Action                                                                                                                                                                                    | Purpose                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                        | Exits from interface configuration mode. |
| Step 10 | <b>mpls ldp session protection</b> [ <b>vrf</b> <i>vpn-name</i> ] [ <b>for</b> <i>acl</i> ] [ <b>duration</b> <i>seconds</i> ]<br><br><b>Example:</b><br>Router(config)# mpls ldp session protection | Enables MPLS LDP Session Protection.     |

## Customizing MPLS LDP Session Protection

You can modify MPLS LDP Session Protection by using the keywords in the **mpls ldp session protection** command. The following sections explain how to customize the feature.

### Specifying How Long an LDP Targeted Hello Adjacency Should Be Retained

The default behavior of the **mpls ldp session protection** command allows an LDP Targeted Hello Adjacency to exist indefinitely following the loss of an LDP Link Hello Adjacency. You can issue the **duration** keyword to specify the number of seconds (from 30 to 2,147,483) that the LDP Targeted Hello Adjacency is retained after the loss of the LDP Link Hello Adjacency. When the link is lost, a timer starts. If the timer expires, the LDP Targeted Hello Adjacency is removed.

### Specifying Which Routers Should Have MPLS LDP Session Protection

The default behavior of the **mpls ldp session protection** command allows MPLS LDP Session Protection for all neighbor sessions. You can issue either the **vrf** or **for** keyword to limit the number of neighbor sessions that are protected.

### Enabling MPLS LDP Session Protection on Specified VPN Routing and Forwarding Instances

If the router is configured with at least one VPN routing and forwarding (VRF) instance, you can use the **vrf** keyword to select which VRF is to be protected. You cannot specify more than one VRF with the **mpls ldp session protection** command. To specify multiple VRFs, issue the command multiple times.

### Enabling MPLS LDP Session Protection on Specified Peer Routers

You can create an access list that includes several peer routers. You can specify that access list with the **for** keyword to enable LDP Session Protection for the peer routers in the access control list.

## Verifying MPLS LDP Session Protection

To verify that LDP Session Protection has been correctly configured, perform the following steps.

### SUMMARY STEPS

1. show mpls ldp discovery
2. show mpls ldp neighbor
3. show mpls ldp neighbor detail

### DETAILED STEPS

#### Step 1 show mpls ldp discovery

Issue this command and check that the output contains xmit/recv to the peer router.

```
Router# show mpls ldp discovery

Local LDP Identifier:
 10.0.0.5:0
Discovery Sources:
Interfaces:
 ATM5/1/0.5 (ldp): xmit/recv
 LDP Id: 10.0.0.1:0
Targeted Hellos:
 10.0.0.5 -> 10.0.0.3 (ldp): active, xmit/recv
 LDP Id: 10.0.0.3:0
```

#### Step 2 show mpls ldp neighbor

Issue this command to check that the targeted hellos are active.

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.0.0.3:0; Local LDP Ident 10.0.0.5:0
TCP connection: 10.0.0.3.646 - 10.0.0.5.11005
State: Oper; Msgs sent/rcvd: 1453/1464; Downstream
Up time: 21:09:56
LDP discovery sources:
 Targeted Hello 10.0.0.5 -> 10.0.0.3, active
Addresses bound to peer LDP Ident:
 10.3.104.3 10.0.0.2 10.0.0.3
```

#### Step 3 show mpls ldp neighbor detail

Issue this command to check that the MPLS LDP Session Protection state is Ready or Protecting. If the second last line of the output shows Incomplete, the Targeted Hello Adjacency is not up yet.

```
Router# show mpls ldp neighbor detail

Peer LDP Ident: 10.16.16.16:0; Local LDP Ident 10.15.15.15:0
TCP connection: 10.16.16.16.11013 - 10.15.15.15.646
State: Oper; Msgs sent/rcvd: 53/51; Downstream; Last TIB rev sent 74
Up time: 00:11:32; UID: 1; Peer Id 0;
LDP discovery sources:
 Targeted Hello 10.15.15.15 -> 10.16.16.16, active, passive;
 holdtime: infinite, hello interval: 10000 ms
Addresses bound to peer LDP Ident:
 10.0.0.2 10.16.16.16 10.101.101.101 11.0.0.1
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
Clients: Dir Adj Client
```

```
LDP Session Protection enabled, state: Protecting
duration: infinite
```

## Troubleshooting Tips

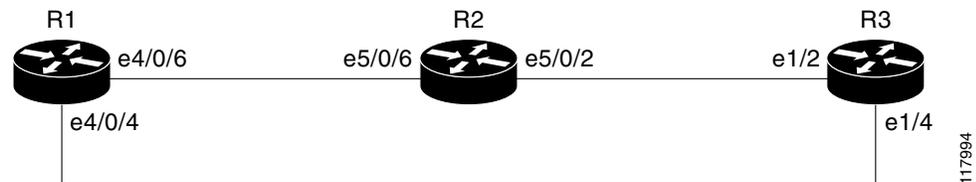
Use the **clear mpls ldp neighbor** command if you need to terminate an LDP session after a link goes down. This is useful for situations where the link needs to be taken out of service or needs to be connected to a different neighbor.

To enable the display of events related to MPLS LDP Session Protection, use the **debug mpls ldp session protection** command.

## Configuration Examples for MPLS LDP Session Protection

Figure 1 shows a sample configuration for MPLS LDP Session Protection.

**Figure 1** *MPLS LDP Session Protection Example*



```
R1
redundancy
 no keepalive-enable
 mode hsa
!
ip cef distributed
no ip domain-lookup
multilink bundle-name both
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
tag-switching tdp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Multilink4
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 ppp multilink
 multilink-group 4
!
interface Ethernet1/0/0
 ip address 10.3.123.1 255.255.0.0
```

```

 no ip directed-broadcast
 !
interface Ethernet4/0/0
 no ip address
 no ip directed-broadcast
 shutdown
 !
interface Ethernet4/0/1
 description -- ip address 10.0.0.2 255.255.255.0
 no ip address
 no ip directed-broadcast
 shutdown
 !
interface Ethernet4/0/4
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 tag-switching ip
 !
interface Ethernet4/0/6
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 tag-switching ip
 !
interface Ethernet4/0/7
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 tag-switching ip
 !
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.1 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 !
ip classless

```

**R2**

```

redundancy
 no keepalive-enable
 mode hsa
 !
ip subnet-zero
ip cef distributed
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
tag-switching tdp router-id Loopback0 force
 !
interface Loopback0
 ip address 10.0.0.3 255.255.255.255
 no ip directed-broadcast
 !
interface Ethernet5/0/0
 no ip address
 no ip directed-broadcast
 shutdown
 full-duplex

```

```
!
interface Ethernet5/0/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 tag-switching ip
!
interface Ethernet5/0/6
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 ip load-sharing per-packet
 full-duplex
 mpls label protocol ldp
 tag-switching ip
!
interface FastEthernet5/1/0
 ip address 10.3.123.112 255.255.0.0
 no ip directed-broadcast
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.3 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

### R3

```
ip cef
no ip domain-lookup
mpls label range 200 100000 static 16 199
mpls label protocol ldp
no mpls traffic-eng auto-bw timers frequency 0
tag-switching tdp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.5 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet1/0
 no ip address
 no ip directed-broadcast
 shutdown
 half-duplex
!
interface Ethernet1/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 tag-switching ip
!
interface Ethernet1/4
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 tag-switching ip
!
router ospf 100
 log-adjacency-changes
```

```
redistribute connected
network 10.0.0.5 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

## Additional References

The following sections provide references related to the MPLS LDP Session Protection feature.

## Related Documents

| Related Topic                | Document Title                                   |
|------------------------------|--------------------------------------------------|
| MPLS LDP                     | <a href="#">MPLS Label Distribution Protocol</a> |
| MPLS LDP-IGP synchronization | <a href="#">MPLS LDP-IGP Synchronization</a>     |
| LDP autoconfiguration        | <a href="#">LDP Autoconfiguration</a>            |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs         | MIBs Link                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS LDP MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title                             |
|----------|-----------------------------------|
| RFC 3036 | <a href="#">LDP Specification</a> |
| RFC 3037 | <a href="#">LDP Applicability</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                       | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls ldp session protection**
- **mpls ldp session protection**
- **show mpls ldp neighbor**
- **Feature Information for MPLS LDP Session Protection**

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS LDP Inbound Label Binding Filtering

---

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) supports inbound label binding filtering. You can use the MPLS LDP feature to configure access control lists (ACLs) for controlling the label bindings a label switch router (LSR) accepts from its peer LSRs.

## History for the MPLS LDP Inbound Label Binding Filtering Feature

| Release     | Modification                                                                                     |
|-------------|--------------------------------------------------------------------------------------------------|
| 12.0(26)S   | This feature was introduced.                                                                     |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S for the Cisco 7500 series router.   |
| 12.3(14)T   | This feature was integrated into Cisco IOS Release 12.3(14)T.                                    |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE for the Cisco 7600 series router. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information about MPLS LDP Inbound Label Binding Filtering, page 2](#)
- [How to Configure MPLS LDP Inbound Label Binding Filtering, page 2](#)
- [Configuration Examples for MPLS LDP Inbound Label Binding Filtering, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 8](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

# Information about MPLS LDP Inbound Label Binding Filtering

The MPLS LDP Inbound Label Binding Filtering feature may be used to control the amount of memory used to store LDP label bindings advertised by other routers. For example, in a simple MPLS Virtual Private Network (VPN) environment, the VPN provider edge (PE) routers may require LSPs only to their peer PE routers (that is, they do not need LSPs to core routers). Inbound label binding filtering enables a PE router to accept labels only from other PE routers.

## How to Configure MPLS LDP Inbound Label Binding Filtering

This section includes the following tasks:

- [Configuring MPLS LDP Inbound Label Binding Filtering, page 2](#) (Required)
- [Verifying that MPLS LDP Inbound Label Bindings are Filtered, page 4](#) (Optional)

## Configuring MPLS LDP Inbound Label Binding Filtering

Perform this task to configure a router for inbound label filtering. The following configuration allows the router to accept only the label for prefix 25.0.0.2 from LDP neighbor router 10.12.12.12.

### Restrictions

Inbound label binding filtering does not support extended ACLs; it only supports standard ACLs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list standard** *access-list-number*
4. **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **exit**
6. **mpls ldp neighbor** [*vrf vpn-name*] *nbr-address* **labels accept** *acl*
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                             | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                | Enters global configuration mode.                                                                                |
| Step 3 | <b>ip access-list standard access-list-number</b><br><br><b>Example:</b><br>Router(config)# ip access-list standard 1                                         | Defines a standard IP access list with a number.                                                                 |
| Step 4 | <b>permit {source [source-wildcard]   any} [log]</b><br><br><b>Example:</b><br>Router(config-std-nacl)# permit 10.0.0.0                                       | Specifies one or more prefixes permitted by the access list.                                                     |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-std-nacl)# exit                                                                                           | Exits the current mode and goes to the next higher level.                                                        |
| Step 6 | <b>mpls ldp neighbor [vrf vpn-name] nbr-address labels accept acl</b><br><br><b>Example:</b><br>Router(config)# mpls ldp neighbor 10.12.12.12 labels accept 1 | Specifies the ACL to be used to filter label bindings for the specified LDP neighbor.                            |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                      | Exits the current mode and enters privileged Exec mode.                                                          |

## Verifying that MPLS LDP Inbound Label Bindings are Filtered

If inbound filtering is enabled, perform the following steps to verify that inbound label bindings are filtered:

- Step 1** Enter the **show mpls ldp neighbor** command to show the status of the LDP session, including the name or number of the ACL configured for inbound filtering.

```
show mpls ldp neighbor [vrf vpn-name][address | interface] [detail]
```



**Note** To display information about inbound label binding filtering, you must enter the **detail** keyword.

Following is sample output from the **show mpls ldp neighbor** command.

```
Router# show mpls ldp neighbor 10.12.12.12 detail

Peer LDP Ident: 10.12.12.12:0; Local LDP Ident 10.13.13.13:0
TCP connection: 10.12.12.12.646 - 10.13.13.13.12592
State: Oper; Msgs sent/rcvd: 49/45; Downstream; Last TIB rev sent 1257
Up time: 00:32:41; UID: 1015; Peer Id 0;
LDP discovery sources:
 Serial1/0; Src IP addr: 25.0.0.2
 holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
 10.0.0.129 10.12.12.12 10.0.0.2
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
LDP inbound filtering accept acl: 1
```

- Step 2** Enter the **show ip access-list** command to display the contents of all current IP access lists or of a specified access list.

```
show ip access-list [access-list-number | access-list-name]
```



**Note** It is important that you enter this command to see how the access list is defined; otherwise, you cannot verify inbound label binding filtering.

*The following command output shows the contents of IP access list 1:*

```
Router# show ip access 1

Standard IP access list 1
 permit 10.0.0.0, wildcard bits 0.0.0.255 (1 match)
```

- Step 3** Enter the **show mpls ldp bindings** command to verify that the LSR has remote bindings only from a specified peer for prefixes permitted by the access list.

```
Router# show mpls ldp bindings

tib entry: 10.0.0.0/8, rev 4
 local binding: tag: imp-null
tib entry: 10.2.0.0/16, rev 1137
 local binding: tag: 16
tib entry: 10.2.0.0/16, rev 1139
 local binding: tag: 17
tib entry: 10.12.12.12/32, rev 1257
 local binding: tag: 18
tib entry: 10.13.13.13/32, rev 14
 local binding: tag: imp-null
```

```
tib entry: 10.10.0.0/16, rev 711
 local binding: tag: imp-null
tib entry: 10.0.0.0/8, rev 1135
 local binding: tag: imp-null
 remote binding: tsr: 12.12.12.12:0, tag: imp-null
tib entry: 10.0.0.0/8, rev 8
 local binding: tag: imp-null
Router#
```

---

## Configuration Examples for MPLS LDP Inbound Label Binding Filtering

In the following example, the **mpls ldp neighbor labels accept** command is configured with an access control list to filter label bindings received on sessions with the neighbor 10.110.0.10.

Label bindings for prefixes that match 10.b.c.d are accepted, where b is less than or equal to 63, and c and d can be any integer between 0 and 128. Other label bindings received from 10.110.0.10 are rejected.

```
Router# configure terminal
Router(config)# access-list 1 permit 10.63.0.0 0.63.255.255
Router(config)# mpls ldp neighbor 10.110.0.10 labels accept 1
Router(config)# end
```

In the following example, the **show mpls ldp bindings neighbor** command displays label bindings that were learned from 10.110.0.10. This example verifies that the LIB does not contain label bindings for prefixes that have been excluded.

```
Router# show mpls ldp bindings neighbor 10.110.0.10

tib entry: 10.2.0.0/16, rev 4
 remote binding: tsr: 10.110.0.10:0, tag: imp-null
tib entry: 10.43.0.0/16, rev 6
 remote binding: tsr: 10.110.0.10:0, tag: 16
tib entry: 10.52.0.0/16, rev 8
 remote binding: tsr: 10.110.0.10:0, tag: imp-null
```

## Additional References

The following sections provide additional references related to MPLS LDP inbound label binding filters.

## Related Documents

| Related Topic                          | Document Title                                   |
|----------------------------------------|--------------------------------------------------|
| MPLS Label Distribution Protocol (LDP) | <a href="#">MPLS Label Distribution Protocol</a> |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB                                                  | MIBs Link                                                                                                                                                                                                              |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>LDP Specification, draft-ietf-mpls-ldp-08.txt</i> | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                             |
|----------|-----------------------------------|
| RFC 3036 | <a href="#">LDP Specification</a> |
| RFC 3037 | <a href="#">LDP Applicability</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- `clear mpls ldp neighbor`

- `mpls ldp neighbor labels accept`
- `show mpls ldp neighbor`

# Glossary

**carrier supporting carrier**—A situation where one service provider allows another service provider 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.

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

**inbound label binding filtering**—Allows LSRs to control which label bindings it will accept from its neighboring LSRs. Consequently, an LSR does not accept or store some label bindings that its neighbors advertise.

**label**—A short fixed-length identifier that tells switching nodes how to forward data (packets or cells).

**label binding**—An association between a destination prefix and a label.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS LDP Autoconfiguration

---

**First Published: November 8, 2004**

**Last Updated: February 20, 2007**

The MPLS LDP Autoconfiguration feature enables you to globally configure Label Distribution Protocol (LDP) on every interface associated with a specified Interior Gateway Protocol (IGP) instance.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To access links to specific feature documentation in this module and to view a list of releases in which each feature is supported, use the “[Feature Information for MPLS LDP Autoconfiguration](#)” section on page 14.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Restrictions for MPLS LDP Autoconfiguration, page 1](#)
- [Information About MPLS LDP Autoconfiguration, page 2](#)
- [How to Configure MPLS LDP Autoconfiguration, page 2](#)
- [Configuration Examples for MPLS LDP Autoconfiguration, page 9](#)
- [Additional References, page 11](#)
- [Command Reference, page 12](#)
- [Feature Information for MPLS LDP Autoconfiguration, page 14](#)

## Restrictions for MPLS LDP Autoconfiguration

This feature has the following restrictions:



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- In Cisco IOS Release 12.2(33)SRB, the MPLS LDP Autoconfiguration feature is supported only with Open Shortest Path First (OSPF). Intermediate System to Intermediate System (IS-IS) is not supported.
- In Cisco IOS Release 12.0(32)SY, the **mpls ldp autoconfig** command is supported with OSPF and IS-IS interfaces. Other IGPs are not supported.
- If LDP is disabled globally, the **mpls ldp autoconfig** command fails and generates a console message explaining that LDP must first be enabled globally by means of the global **mpls ip** command.
- If the **mpls ldp autoconfig** command is configured for an IGP instance, you cannot issue the global **no mpls ip** command. To disable LDP, you must first issue the **no mpls ldp autoconfig** command.
- For interfaces running IS-IS processes, you can enable Multiprotocol Label Switching (MPLS) for each interface, using the router mode command **mpls ldp autoconfig** or **mpls ldp igp autoconfig** at the interface level.
- You specify that the default label distribution protocol is LDP for a router or for an interface. Tag Distribution Protocol (TDP) is not supported.
- The MPLS LDP Autoconfiguration feature is not supported on traffic engineering tunnel interfaces.

## Information About MPLS LDP Autoconfiguration

To enable LDP, you should configure it globally and on each interface where it is needed. Configuring LDP on many interfaces can be time consuming.

The MPLS LDP Autoconfiguration feature enables you to globally enable LDP on every interface associated with an IGP instance. This feature is supported on OSPF and IS-IS IGPs. Further, it provides a means to block LDP from being enabled on interfaces that you do not want enabled. The goal of the MPLS LDP Autoconfiguration feature is to make configuration easier, faster, and error free.



### Note

---

In Cisco IOS Release 12.2(33)SRB, the MPLS LDP Autoconfiguration feature is supported only with OSPF. IS-IS is not supported.

---

You issue the **mpls ldp autoconfig** command to enable LDP on each interface that is running an OSPF or IS-IS process. If you do not want some of the interfaces to have LDP enabled, you can issue the **no** form of the **mpls ldp igp autoconfig** command on those interfaces.

## How to Configure MPLS LDP Autoconfiguration

This section contains the following procedures:

- [Configuring MPLS LDP Autoconfiguration with OSPF Interfaces, page 3](#) (required)
- [Disabling MPLS LDP Autoconfiguration from Selected OSPF Interfaces, page 4](#) (optional)
- [Verifying MPLS LDP Autoconfiguration with OSPF, page 5](#) (optional)
- [Configuring MPLS LDP Autoconfiguration with IS-IS Interfaces, page 6](#) (required)
- [Disabling MPLS LDP Autoconfiguration from Selected IS-IS Interfaces, page 8](#) (optional)
- [Verifying MPLS LDP Autoconfiguration with IS-IS, page 9](#) (optional)

## Configuring MPLS LDP Autoconfiguration with OSPF Interfaces

The following steps explain how to configure LDP for interfaces running OSPF processes.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol ldp**
5. **interface *interface***
6. **ip address *prefix mask***
7. **exit**
8. **router ospf *process-id***
9. **network *ip-address wildcard-mask area area-id***
10. **mpls ldp autoconfig [*area area-id*]**

### DETAILED STEPS

|        | Command or Action                                                                                | Purpose                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                   | Enters global configuration mode.                                                                                     |
| Step 3 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip                                 | Globally enables hop-by-hop forwarding.                                                                               |
| Step 4 | <b>mpls label protocol ldp</b><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp | Specifies LDP as the default label distribution protocol.                                                             |
| Step 5 | <b>interface <i>interface</i></b><br><br><b>Example:</b><br>Router(config)# interface POS3/0     | Specifies the interface to configure and enters interface configuration mode.                                         |

|         | Command or Action                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                         |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <code>ip address prefix mask</code><br><br><b>Example:</b><br>Router(config-if)# ip address 10.0.0.11<br>255.255.255.255                           | Assigns an IP address to the interface.                                                                                                                                                                                                                                                                         |
| Step 7  | <code>exit</code><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                | Exits interface configuration mode.                                                                                                                                                                                                                                                                             |
| Step 8  | <code>router ospf process-id</code><br><br><b>Example:</b><br>Router(config)# router ospf 1                                                        | Enables OSPF routing and enters router configuration mode.                                                                                                                                                                                                                                                      |
| Step 9  | <code>network ip-address wildcard-mask area area-id</code><br><br><b>Example:</b><br>Router(config-router)# network 10.0.0.0<br>0.0.255.255 area 3 | Specifies the interface on which OSPF runs and defines the area ID for that interface.                                                                                                                                                                                                                          |
| Step 10 | <code>mpls ldp autoconfig [area area-id]</code><br><br><b>Example:</b><br>Router(config-router)# mpls ldp autoconfig area<br>3                     | Enables the MPLS LDP Autoconfiguration feature to enable LDP on interfaces belonging to an OSPF process. If no area is specified, the command applies to all interfaces associated with the OSPF process. If an area ID is specified, then only interfaces associated with that OSPF area are enabled with LDP. |

## Disabling MPLS LDP Autoconfiguration from Selected OSPF Interfaces

When you issue the `mpls ldp autoconfig` command, all the interfaces that belong to an OSPF area are enabled for LDP. To remove LDP from some interfaces, use the `no mpls ldp igp autoconfig` command on those interfaces. The following configuration steps show how to disable LDP from some of the interfaces after they were configured with MPLS LDP Autoconfiguration with the `mpls ldp autoconfig` command.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface`
4. `no mpls ldp igp autoconfig`

## DETAILED STEPS

|        | Command or Action                                                                                         | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                            | Enters global configuration mode.                                                                                |
| Step 3 | <b>interface interface</b><br><br><b>Example:</b><br>Router(config)# interface POS3/0                     | Specifies the interface to configure and enters interface configuration mode.                                    |
| Step 4 | <b>no mpls ldp igp autoconfig</b><br><br><b>Example:</b><br>Router(config-if)# no mpls ldp igp autoconfig | Disables LDP for that interface.                                                                                 |

## Verifying MPLS LDP Autoconfiguration with OSPF

The following steps explain how to verify the MPLS LDP Autoconfiguration feature.

### SUMMARY STEPS

1. **show mpls interfaces [detail]**
2. **show mpls ldp discovery [detail]**

### DETAILED STEPS

#### Step 1 **show mpls interfaces**

The **show mpls interfaces** command lists the method that was used to enable LDP on an interface.

- If LDP is enabled by the **mpls ldp autoconfig** command, the output displays:

```
IP labeling enabled (ldp):
 IGP config
```

- If LDP is enabled by the **mpls ip** command, the output displays:

```
IP labeling enabled (ldp):
 Interface config
```

- If LDP is enabled by the **mpls ip** command and the **mpls ldp autoconfig** command, the output displays:

```
IP labeling enabled (ldp):
 Interface config
 IGP config
```

The following example shows that LDP was enabled on the interface by both the **mpls ip** and **mpls ldp autoconfig** commands:

```
Router# show mpls interfaces S2/0 detail

Interface Serial2/0:
 IP labeling enabled (ldp):
 Interface config
 IGP config
 LSP Tunnel labeling enabled
 BGP labeling not enabled
 MPLS operational
 Fast Switching Vectors:
 IP to MPLS Fast Switching Vector
 MPLS Turbo Vector
 MTU = 1500
```

### Step 2 show mpls ldp discovery

The **show mpls ldp discovery details** command also show how LDP was enabled on the interface. In the following example, LDP was enabled by both the **mpls ip** and **mpls ldp autoconfig** commands:

```
Router# show mpls ldp discovery detail

Local LDP Identifier:
 10.11.11.11:0
 Discovery Sources:
 Interfaces:
 Serial2/0 (ldp): xmit/recv
 Enabled: Interface config, IGP config;
 Hello interval: 5000 ms; Transport IP addr: 10.11.11.11
 LDP Id: 10.10.10.10:0
 Src IP addr: 10.0.0.1; Transport IP addr: 10.10.10.10
 Hold time: 15 sec; Proposed local/peer: 15/15 sec
```

## Configuring MPLS LDP Autoconfiguration with IS-IS Interfaces

The following steps explain how to configure the MPLS LDP Autoconfiguration feature for interfaces running IS-IS processes.



### Note

In Cisco IOS Release 12.2(33)SRB, the MPLS LDP Autoconfiguration feature is supported only with OSPF. IS-IS is not supported.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface*
4. **ip address** *prefix mask*
5. **ip router isis**
6. **exit**
7. **mpls ip**

8. `mpls label protocol ldp`
9. `router isis`
10. `mpls ldp autoconfig` [*level-1* | *level-2*]

## DETAILED STEPS

|        | Command or Action                                                                                                            | Purpose                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><code>enable</code></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <p><code>configure terminal</code></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                 | <p>Enters global configuration mode.</p>                                                                                  |
| Step 3 | <p><code>interface interface</code></p> <p><b>Example:</b><br/>Router(config)# interface POS0/2</p>                          | <p>Specifies the interface to configure and enters interface configuration mode.</p>                                      |
| Step 4 | <p><code>ip address prefix mask</code></p> <p><b>Example:</b><br/>Router(config-if)# ip address 10.50.72.4<br/>255.0.0.0</p> | <p>Assigns an IP address to the interface.</p>                                                                            |
| Step 5 | <p><code>ip router isis</code></p> <p><b>Example:</b><br/>Router(config-if)# ip router isis</p>                              | <p>Enables IS-IS for IP on the interface.</p>                                                                             |
| Step 6 | <p><code>exit</code></p> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                  | <p>Exits interface configuration mode.</p>                                                                                |
| Step 7 | <p><code>mpls ip</code></p> <p><b>Example:</b><br/>Router(config)# mpls ip</p>                                               | <p>Globally enables hop-by-hop forwarding.</p>                                                                            |
| Step 8 | <p><code>mpls label protocol ldp</code></p> <p><b>Example:</b><br/>Router(config)# mpls label protocol ldp</p>               | <p>Specifies LDP as the default label distribution protocol.</p>                                                          |

|         | Command or Action                                                                                                                      | Purpose                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Step 9  | <code>router isis</code><br><br><b>Example:</b><br><code>Router(config)# router isis</code>                                            | Enables an IS-IS process on the router and enters router configuration mode. |
| Step 10 | <code>mpls ldp autoconfig [level-1   level-2]</code><br><br><b>Example:</b><br><code>Router(config-router)# mpls ldp autoconfig</code> | Enables the LDP for interfaces belonging to an IS-IS process.                |

## Disabling MPLS LDP Autoconfiguration from Selected IS-IS Interfaces

When you issue the `mpls ldp autoconfig` command, all the interfaces that belong to an IS-IS process are enabled for LDP. To remove LDP from some interfaces, you can use the `no` form of the `mpls ldp igp autoconfig` command on those interfaces. The following configuration steps show how to disable LDP from some of the interfaces after they were configured with the MPLS LDP Autoconfiguration through the `mpls ldp autoconfig` command.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface`
4. `no mpls ldp igp autoconfig`

### DETAILED STEPS

|        | Command or Action                                                                                                            | Purpose                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code>                            | Enters global configuration mode.                                                                                  |
| Step 3 | <code>interface interface</code><br><br><b>Example:</b><br><code>Router(config)# interface POS3/0</code>                     | Specifies the interface to configure and enters interface configuration mode.                                      |
| Step 4 | <code>no mpls ldp igp autoconfig</code><br><br><b>Example:</b><br><code>Router(config-if)# no mpls ldp igp autoconfig</code> | Disables LDP for that interface.                                                                                   |

## Verifying MPLS LDP Autoconfiguration with IS-IS

You can verify that the MPLS LDP Autoconfiguration feature is working correctly with the **show isis mpls ldp** command.

### SUMMARY STEPS

1. **enable**
2. **show isis mpls ldp**

### DETAILED STEPS

---

**Step 1 enable**

Enables privileged EXEC mode.

**Step 2 show isis mpls ldp**

The output of the following **show isis mpls ldp** command shows that IS-IS is configured on the interface and LDP is enabled:

```
Router# show isis mpls ldp

Interface: POS0/2; ISIS tag null enabled
ISIS is UP on interface
AUTOCONFIG Information :
 LDP enabled: YES
 SYNC Information :
 Required: NO
```

The output shows :

- IS-IS is up.
- LDP is enabled.

If the MPLS LDP Autoconfiguration feature is not enabled on an interface, the output looks like the following:

```
Interface: Ethernet0; ISIS tag null enabled
ISIS is UP on interface
AUTOCONFIG Information :
 LDP enabled: NO
 SYNC Information :
 Required: NO
```

---

### Troubleshooting Tips

You can use the **debug mpls ldp autoconfig** command to display events related to the MPLS LDP Autoconfiguration feature.

## Configuration Examples for MPLS LDP Autoconfiguration

The following sections show examples for MPLS LDP Autoconfiguration with OSPF and IS-IS processes.

- [MPLS LDP Autoconfiguration Examples with OSPF, page 10](#)
- [MPLS LDP Autoconfiguration Examples with IS-IS, page 10](#)

## MPLS LDP Autoconfiguration Examples with OSPF

The following configuration commands enable LDP for OSPF process 1 area 3. The **mpls ldp autoconfig area 3** command and the OSPF **network** commands enable LDP on interfaces POS0/0, POS0/1, and POS1/1. The **no mpls ldp igp autoconfig** command on interface POS1/0 prevents LDP from being enabled on interface POS1/0, even though OSPF is enabled for that interface.

```
configure terminal
interface POS0/0
 ip address 10.0.0.1
!
interface POS0/1
 ip address 10.0.1.1
!
interface POS1/1
 ip address 10.1.1.1
!
interface POS1/0
 ip address 10.1.0.1
 exit
!
router ospf 1
 network 10.0.0.0 0.0.255.255 area 3
 network 10.1.0.0 0.0.255.255 area 3
 mpls ldp autoconfig area 3
 exit
interface POS1/0
 no mpls ldp igp autoconfig
```

## MPLS LDP Autoconfiguration Examples with IS-IS



### Note

In Cisco IOS Release 12.2(33)SRB, MPLS LDP Autoconfiguration is supported only with OSPF. IS-IS is not supported.

The following example shows the configuration of MPLS LDP Autoconfiguration on interfaces POS0/2 and POS0/3, which are running IS-IS processes:

```
configure terminal
interface POS0/2
 ip address 10.0.0.1
 ip router isis
!
interface POS0/3
 ip address 10.1.1.1
 ip router isis
 exit

mpls ip
mpls label protocol ldp
router isis
 mpls ldp autoconfig
```

# Additional References

The following sections provide references related to the MPLS LDP Autoconfiguration feature.

## Related Documents

| Related Topic                            | Document Title                                                    |
|------------------------------------------|-------------------------------------------------------------------|
| MPLS LDP                                 | <a href="#"><i>MPLS Label Distribution Protocol</i></a>           |
| The MPLS LDP-IGP Synchronization feature | <a href="#"><i>MPLS LDP-IGP Synchronization</i></a>               |
| The MPLS LDP Session Protection feature  | <a href="#"><i>MPLS LDP Session Protection</i></a>                |
| Configuring integrated IS-IS             | <a href="#"><i>Integrated IS-IS Routing Protocol Overview</i></a> |

## Standards

| Standard                                                                                                                             | Title |
|--------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature | —     |

## MIBs

| MIB          | MIBs Link                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS LDP MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                             |
|----------|-----------------------------------|
| RFC 3036 | <a href="#">LDP Specification</a> |
| RFC 3037 | <a href="#">LDP Applicability</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                       | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls ldp autoconfig**
- **mpls ldp autoconfig**

- **mpls ldp igp autoconfig**
- **show isis mpls ldp**
- **show mpls ldp discovery**

# Feature Information for MPLS LDP Autoconfiguration

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS LDP Autoconfiguration

| Feature Name               | Releases                                                          | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS LDP Autoconfiguration | 12.0(30)S<br>12.3(14)T<br>12.2(28)SB<br>12.0(32)SY<br>12.2(33)SRB | <p>This feature enables you to globally configure LDP on every interface associated with a specified Interior Gateway Protocol (IGP) instance.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About MPLS LDP Autoconfiguration, page 2</a></li> <li>• <a href="#">How to Configure MPLS LDP Autoconfiguration, page 2</a></li> </ul> <p>In Cisco IOS Release 12.2(32)SY, support for IS-IS was added.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB. The MPLS LDP Autoconfiguration feature is not supported with IS-IS in this release.</p> |

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS LDP Graceful Restart

---

When a router is configured with Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Graceful Restart (GR), it assists a neighboring router that has MPLS LDP Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart to recover gracefully from an interruption in service. In this Cisco IOS release, MPLS LDP GR functions strictly in helper mode, which means it can only help other routers that are enabled with MPLS SSO/NSF and GR to recover. If the router with LDP GR fails, its peer routers cannot help it recover.

## Notes:

- MPLS LDP SSO/NSF Support and Graceful Restart is supported in Cisco IOS Release 12.2(25)S. For brevity, this feature is called LDP SSO/NSF in this document.
- The MPLS LDP GR feature described in this document refers to helper mode.

When you enable MPLS LDP GR on a router that peers with an MPLS LDP SSO/NSF-enabled router, the SSO/NSF-enabled router can maintain its forwarding state when the LDP session between them is interrupted. While the SSO/NSF-enabled router recovers, the peer router forwards packets using stale information. This enables the SSO/NSF-enabled router to become operational more quickly.

## Feature History for MPLS LDP Graceful Restart

| Release                  | Modification                                                           |
|--------------------------|------------------------------------------------------------------------|
| 12.0(29)S                | The MPLS LDP Graceful Restart feature (in helper mode) was introduced. |
| 12.3(14)T                | This feature was integrated into Cisco IOS Release 12.3(14)T.          |
| 12.2(33)SRA              | This feature was integrated into Cisco IOS Release 12.2(33)SRA.        |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.          |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Information About MPLS LDP Graceful Restart, page 2](#)
- [How to Configure MPLS LDP Graceful Restart, page 3](#)
- [Configuration Example for MPLS LDP Graceful Restart, page 6](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)

## Information About MPLS LDP Graceful Restart

To configure MPLS LDP GR, you need to understand the following concepts:

- [How MPLS LDP Graceful Restart Works, page 2](#)
- [How a Route Processor Advertises That It Supports MPLS LDP Graceful Restart, page 3](#)
- [What Happens If a Route Processor Does Not Have LDP Graceful Restart, page 3](#)

## How MPLS LDP Graceful Restart Works

MPLS LDP GR works in strict helper mode, which means it helps a neighboring route processor that has MPLS LDP SSO/NSF to recover from disruption in service without losing its MPLS forwarding state. The disruption in service could be the result of a TCP or UDP event or the stateful switchover of a route processor. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding states are recovered.

In the topology shown in [Figure 1](#), the following elements have been configured:

- LDP sessions are established between Router 1 and Router 2, as well as between Router 2 and Router 3.
- Router 2 has been configured with MPLS LDP SSO/NSF. Routers 1 and 3 have been configured with MPLS LDP GR.
- A label switched path (LSP) has been established between Router 1 and Router 3.

**Figure 1**      *Example of a Network Using LDP Graceful Restart*



The following process shows how Routers 1 and 3, which have been configured with LDP GR help Router 2, which has been configured with LDP SSO/NSF recover from a disruption in service:

1. Router 1 notices an interruption in service with Router 2. (Router 3 also performs the same actions in this process.)
2. Router 1 marks all the label bindings from Router 2 as stale, but it continues to use the bindings for MPLS forwarding.

Router 1 reestablishes an LDP session with Router 2, but keeps its stale label bindings. If you issue a **show mpls ldp neighbor** command with the **graceful-restart** keyword, the command output displays the recovering LDP sessions.

- Both routers readvertise their label binding information. If Router 1 relearns a label from Router 2 after the session has been established, the stale flags are removed. The **show mpls forwarding-table** command displays the information in the MPLS forwarding table, including the local label, outgoing label or VC, prefix, label-switched bytes, outgoing interface, and next hop.

You can set various graceful restart timers. See the following commands for more information:

- mpls ldp graceful-restart timers neighbor-liveness**
- mpls ldp graceful-restart timers max-recovery**

## How a Route Processor Advertises That It Supports MPLS LDP Graceful Restart

A route processor that is configured to perform MPLS LDP GR includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The route processor sends the LDP initialization message to a neighbor to establish an LDP session.

The FT session TLV includes the following information:

- The Learn from Network (L) flag is set to 1, which indicates that the route processor is configured to perform MPLS LDP GR.
- The Reconnect Timeout field shows the time (in milliseconds) that the neighbor should wait for a reconnection if the LDP session is lost. In this release, the timer is set to 0, which indicates that if the local router fails, its peers should not wait for it to recover. The timer setting indicates that the local router is working in helper mode.
- The Recovery Time field shows the time (in milliseconds) that the neighbor should retain the MPLS forwarding state during a recovery. If a neighbor did not preserve the MPLS forwarding state before the restart of the control plane, the neighbor sets the recovery time to 0.

## What Happens If a Route Processor Does Not Have LDP Graceful Restart

If two route processors establish an LDP session and one route processor is not configured for MPLS LDP GR, the two route processors create a normal LDP session but do not have the ability to perform MPLS LDP GR. Both route processors must be configured for MPLS LDP GR.

## How to Configure MPLS LDP Graceful Restart

This section contains the following procedures:

- [Configuring MPLS LDP Graceful Restart, page 3](#) (required)
- [Verifying the Configuration, page 5](#) (optional)

## Configuring MPLS LDP Graceful Restart

You must enable MPLS LDP GR on all route processors for an LDP session to be preserved during an interruption in service.

MPLS LDP GR is enabled globally. When you enable MPLS LDP GR, it has no effect on existing LDP sessions. New LDP sessions that are established can perform MPLS LDP GR.

## Restrictions

- MPLS LDP GR is supported in strict helper mode.
- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS LDP GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.
- MPLS LDP SSO/NSF is supported in IOS Release 12.2(25)S. It is not supported in this release.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **mpls ldp graceful-restart**
5. **interface type slot/port**
6. **mpls ip**
7. **mpls label protocol {ldp | tdp | both}**

## DETAILED STEPS

|        | Command or Action                                                                                    | Purpose                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                       | Enters global configuration mode.                                                                                  |
| Step 3 | <b>ip cef [distributed]</b><br><br><b>Example:</b><br>Router(config)# ip cef distributed             | Enables Cisco Express Forwarding (CEF).                                                                            |
| Step 4 | <b>mpls ldp graceful-restart</b><br><br><b>Example:</b><br>Router(config)# mpls ldp graceful-restart | Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.           |
| Step 5 | <b>interface type slot/port</b><br><br><b>Example:</b><br>Router(config)# interface pos 3/0          | Specifies an interface and enters interface configuration mode.                                                    |

|        | Command or Action                                                                                                                     | Purpose                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Step 6 | <code>mpls ip</code><br><br><b>Example:</b><br>Router(config-if)# <code>mpls ip</code>                                                | Configures MPLS hop-by-hop forwarding for an interface.       |
| Step 7 | <code>mpls label protocol {ldp   tdp   both}</code><br><br><b>Example:</b><br>Router(config-if)# <code>mpls label protocol ldp</code> | Configures the use of LDP for an interface. You must use LDP. |

**Note**

You can also issue the `mpls label protocol ldp` command in global configuration mode, which enables LDP on all interfaces configured for MPLS.

## Verifying the Configuration

The following commands help verify that MPLS LDP GR has been configured correctly:

|                                                                       |                                                             |
|-----------------------------------------------------------------------|-------------------------------------------------------------|
| <code>show mpls ldp neighbor with the graceful-restart keyword</code> | Displays the Graceful Restart information for LDP sessions. |
| <code>show mpls ldp graceful-restart</code>                           | Displays Graceful Restart sessions and session parameters.  |

# Configuration Example for MPLS LDP Graceful Restart

Figure 2 shows a configuration where MPLS LDP GR is enabled on Router 1 and MPLS LDP SSO/NSF is enabled on Routers 2 and 3. In this configuration example, Router 1 creates an LDP session with Router 2. Router 1 also creates a targeted session with Router 3 through a traffic engineering tunnel using Router 2.


**Note**

MPLS LDP SSO/NSF is supported in Cisco IOS Release 12.2(25)S. It is not supported in this release.

**Figure 2** *MPLS LDP Graceful Restart Configuration Example*


**Router 1 configured with LDP GR:**

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
ip subnet-zero
ip cef
mpls label range 16 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 20.20.20.20 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnell
 ip unnumbered Loopback0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
 tunnel destination 19.19.19.19
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface ATM5/1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
```

```

 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 !
interface ATM5/1/0.5 point-to-point
 ip address 12.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
 encapsulation aal5snap
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 12.0.0.0 0.255.255.255 area 100
 network 20.20.20.20 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100

```

#### Router 2 configured with LDP SSO/NSF:

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
redundancy
 mode sso
!
ip cef
no ip domain-lookup
mpls label range 17 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
no mpls advertise-labels
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 17.17.17.17 255.255.255.255
 no ip directed-broadcast
!
interface ATM4/0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
 ip address 12.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
 encapsulation aal5snap
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip

```

```

 ip rsvp bandwidth 1000
 !
interface POS5/1/0
 ip address 11.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 nsf enforce global
 network 11.0.0.0 0.255.255.255 area 100
 network 12.0.0.0 0.255.255.255 area 100
 network 17.17.17.17 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless

```

### Router 3 configured with LDP SSO/NSF:

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
redundancy
 mode sso
!
ip subnet-zero
ip cef
!
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp neighbor 11.11.11.11 targeted ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery directed-hello interval 12
mpls ldp discovery directed-hello holdtime 130
mpls ldp discovery directed-hello accept
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 19.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface POS1/0
 ip address 11.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000

```

```
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 nsf enforce global
 network 11.0.0.0 0.255.255.255 area 100
 network 19.19.19.19 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

## Additional References

The following sections provide references related to MPLS LDP GR.

### Related Documents

| Related Topic                    | Document Title                                         |
|----------------------------------|--------------------------------------------------------|
| MPLS Label Distribution Protocol | <a href="#">MPLS Label Distribution Protocol (LDP)</a> |

### Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

### MIBs

| MIBs <sup>1</sup>                                                                                        | MIBs Link                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>MPLS Label Distribution Protocol MIB Version 8 Upgrade</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

1. Not all supported MIBs are listed.

### RFCs

| RFCs <sup>1</sup> | Title                                                    |
|-------------------|----------------------------------------------------------|
| RFC 3036          | <i>LDP Specification</i>                                 |
| RFC 3478          | <i>Graceful Restart Mechanism for Label Distribution</i> |

1. Not all supported RFCs are listed.

### Technical Assistance

| Description                                                                                                                                                                                                                                                                                    | Link                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Technical Support &amp; Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls ldp graceful-restart**
- **mpls ldp graceful-restart**
- **mpls ldp graceful-restart timers max-recovery**
- **mpls ldp graceful-restart timers neighbor-liveness**
- **show mpls ip binding**
- **show mpls ldp bindings**
- **show mpls ldp graceful-restart**
- **show mpls ldp neighbor**



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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS Label Distribution Protocol MIB Version 8 Upgrade

**First Published: November 13, 2000**

**Last Updated: June 29, 2007**

The MPLS Label Distribution Protocol (LDP) MIB Version 8 Upgrade feature enhances the LDP MIB to support the Internet Engineering Task Force (IETF) draft Version 8.

## History for MPLS Label Distribution Protocol MIB Version 8 Update Feature

| Release     | Modification                                                                                                                                                                       |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(11)ST  | This feature was introduced to provide SNMP agent support for the MPLS LDP MIB on Cisco 7200, Cisco 7500, and Cisco 12000 series routers.                                          |
| 12.2(2)T    | This feature was added to this release to provide SNMP agent support for the MPLS LDP MIB on Cisco 7200 and Cisco 7500 series routers.                                             |
| 12.0(21)ST  | This feature was added to this release to provide SNMP agent and LDP notification support for the MPLS LDP MIB on Cisco 7200, Cisco 7500, and Cisco 12000 series Internet routers. |
| 12.0(22)S   | This feature (Version 1) was integrated into Cisco IOS Release 12.0(22)S.                                                                                                          |
| 12.0(24)S   | This feature was upgraded to Version 8 in Cisco IOS Release 12.0(24)S.                                                                                                             |
| 12.0(27)S   | Support for the MPLS VPN—VPN Aware LDP MIB feature was added.                                                                                                                      |
| 12.2(18)S   | This feature was integrated into Cisco IOS Release 12.2(18)S.                                                                                                                      |
| 12.2(33)SRA | This feature was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                    |
| 12.2(33)SXH | This feature was integrated into Cisco IOS Release 12.2(33)SXH.                                                                                                                    |

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for MPLS LDP MIB Version 8 Upgrade, page 2](#)
- [Restrictions for MPLS LDP MIB Version 8 Upgrade, page 2](#)
- [Information About MPLS LDP MIB Version 8 Upgrade, page 3](#)
- [Description of MPLS LDP MIB Elements for MPLS LDP MIB Version 8 Upgrade, page 5](#)
- [Events Generating MPLS LDP MIB Notifications in MPLS LDP MIB Version 8 Upgrade, page 9](#)
- [MIB Tables in MPLS LDP MIB Version 8 Upgrade, page 10](#)
- [VPN Contexts in MPLS LDP MIB Version 8 Upgrade, page 20](#)
- [How to Configure MPLS LDP MIB Version 8 Upgrade, page 24](#)
- [Configuration Examples for MPLS LDP MIB Version 8 Upgrade, page 36](#)
- [Additional References, page 38](#)
- [Command Reference, page 40](#)
- [Glossary, page 42](#)

## Prerequisites for MPLS LDP MIB Version 8 Upgrade

- Simple Network Management Protocol (SNMP) must be installed and enabled on the label switch routers (LSRs).
- Multiprotocol Label Switching (MPLS) must be enabled on the LSRs.
- LDP must be enabled on the LSRs.

## Restrictions for MPLS LDP MIB Version 8 Upgrade

This implementation of the MPLS LDP MIB is limited to read-only (RO) permission for MIB objects, except for MIB object *mplsLdpSessionUpDownTrapEnable*, which has been extended to be writable by the SNMP agent.

Setting this object to a value of true enables both the *mplsLdpSessionUp* and *mplsLdpSessionDown* notifications on the LSR; conversely, setting this object to a value of false disables both of these notifications.

For a description of notification events, see the [“Events Generating MPLS LDP MIB Notifications in MPLS LDP MIB Version 8 Upgrade” section on page 9](#).

Most MPLS LDP MIB objects are set up automatically during the LDP peer discovery (hello) process and the subsequent negotiation of parameters and establishment of LDP sessions between the LDP peers.

The following tables are not implemented in this feature:

- *mplsLdpEntityFrParmsTable*
- *mplsLdpEntityConfFrLRTable*
- *mplsLdpFrameRelaySesTable*
- *mplsFecTable*
- *mplsLdpSesInLabelMapTable*

- `mplsXCsfecsTable`
- `mplsLdpSesPeerAddrTable`

## Information About MPLS LDP MIB Version 8 Upgrade

To configure MPLS LDP MIB Version 8 Upgrade, you need to understand the following concepts:

- [Feature Design of MPLS LDP MIB Version 8 Upgrade, page 3](#)
- [Enhancements in Version 8 of the MPLS LDP MIB, page 4](#)
- [Benefits of MPLS LDP MIB Version 8 Upgrade, page 5](#)

## Feature Design of MPLS LDP MIB Version 8 Upgrade

MPLS is a packet forwarding technology that uses a short, fixed-length value called a label in packets to specify the next hop for packet transport through an MPLS network by means of label switch routers (LSRs).

A fundamental MPLS principle is that LSRs in an MPLS network must agree on the definition of the labels being used for packet forwarding operations. Label agreement is achieved in an MPLS network by means of procedures defined in the LDP.

LDP operations begin with a discovery (hello) process, during which an LDP entity (a local LSR) finds a cooperating LDP peer in the network, and the two negotiate basic operating procedures. The recognition and identification of a peer by means of this discovery process results in a hello adjacency, which represents the context within which label binding information is exchanged between the local LSR and its LDP peer. LDP then creates an active LDP session between the two LSRs to effect the exchange of label binding information. When this process is carried to completion with respect to all of the LSRs in an MPLS network, the result is a label-switched path (LSP), which constitutes an end-to-end packet transmission pathway between the communicating network devices.

By means of LDP, LSRs can collect, distribute, and release label binding information to other LSRs in an MPLS network, thereby enabling the hop-by-hop forwarding of packets in the network along normally routed paths.

The MPLS LDP MIB has been implemented to enable standard, SNMP-based network management of the label switching features in Cisco IOS software. Providing this capability requires SNMP agent code to execute on a designated network management station (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MPLS LDP MIB.

The SNMP agent code has a layered structure that is compatible with Cisco IOS software and presents a network administrative and management interface to the objects in the MPLS LDP MIB and, thence, to the rich set of label switching capabilities supported by Cisco IOS software.

By means of an SNMP agent, you can access MPLS LDP MIB objects using standard SNMP GET operations, and you can use those objects to accomplish a variety of network management tasks. All the objects in the MPLS LDP MIB follow the conventions defined in the IETF draft MIB entitled *draft-ietf-mpls-ldp-mib-08.txt*, which defines network management objects in a structured and standardized manner. This draft MIB is evolving and is soon expected to be a standard. Accordingly, the MPLS LDP MIB will be implemented in such a way that it tracks the evolution of this IETF document.

However, slight differences exist between the IETF draft MIB and the implementation of equivalent Cisco IOS functions. As a result, some minor translations between the MPLS LDP MIB objects and the internal Cisco IOS data structures are needed. Such translations are accomplished by the SNMP agent, which runs in the background on the NMS workstation as a low-priority process.

The extensive Cisco IOS label switching capabilities provide an integrated approach to managing the large volumes of traffic carried by WANs. These capabilities are integrated into the Layer 3 network services, thus optimizing the routing of high-volume traffic through Internet service provider backbones while, at the same time, ensuring the resistance of the network to link or node failures.

Cisco IOS Release 12.0(11)ST and later releases support the following MPLS LDP MIB-related functions:

- Tag Distribution Protocol (TDP)
- Generation and sending of event notification messages that signal changes in the status of LDP sessions
- Enabling and disabling of event notification messages by means of extensions to existing SNMP CLI commands
- Specification of the name or the IP address of an NMS workstation in the operating environment to which Cisco IOS event notification messages are to be sent to serve network administrative and management purposes
- Storage of the configuration pertaining to an event notification message in NVRAM of the NMS

The structure of the MPLS LDP MIB conforms to Abstract Syntax Notation One (ASN.1), so the MIB forms a highly structured and idealized database of network management objects.

Using any standard SNMP application, you can retrieve and display information from the MPLS LDP MIB by means of standard SNMP GET and GETNEXT operations.


**Note**

Because the MPLS LDP MIB was not given an Internet Assigned Numbers Authority (IANA) experimental object identifier (OID) at the time of its implementation, Cisco chose to implement the MIB under the `ciscoExperimental` OID number, as follows:

```
ciscoExperimental
1.3.6.1.4.1.9.10
mplsLdpMIB
1.3.6.1.4.1.9.10.65
```

If the MPLS LDP MIB is assigned an IANA Experimental OID number, Cisco will replace all objects in the MIB under the `ciscoExperimental` OID and reposition the objects under the IANA Experimental OID.

## Enhancements in Version 8 of the MPLS LDP MIB

Version 8 of the MPLS LDP MIB contains the following enhancements:

- TDP support
- Upgraded objects
- New indexing that is no longer based on the number of sessions
- Multiple SNMP context support for Virtual Private Networks (VPNs)

## Benefits of MPLS LDP MIB Version 8 Upgrade

- Supports TDP and LDP
- Establishes LDP sessions between peer devices in an MPLS network
- Retrieves MIB parameters relating to the operation of LDP entities, such as:
  - Well-known LDP discovery port
  - Maximum transmission unit (MTU)
  - Proposed keepalive timer interval
  - Loop detection
  - Session establishment thresholds
  - Range of virtual path identifier/virtual channel identifier (VPI/VCI) pairs to be used in forming labels
- Gathers statistics related to LDP operations, such as error counters ([Table 5](#))
- Monitors the time remaining for hello adjacencies
- Monitors the characteristics and status of LDP peers, such as:
  - Internetwork layer address of LDP peers
  - Loop detection of the LDP peers
  - Default MTU of the LDP peer
  - Number of seconds the LDP peer proposes as the value of the keepalive interval
- Monitors the characteristics and status of LDP sessions, such as:
  - Displaying the error counters ([Table 10](#))
  - Determining the LDP version being used by the LDP session
  - Determining the keepalive hold time remaining for an LDP session
  - Determining the state of an LDP session (whether the session is active or not)
  - Displaying the label ranges ([Table 2](#)) for platform-wide and interface-specific sessions
  - Displaying the ATM parameters ([Table 3](#))

## Description of MPLS LDP MIB Elements for MPLS LDP MIB Version 8 Upgrade

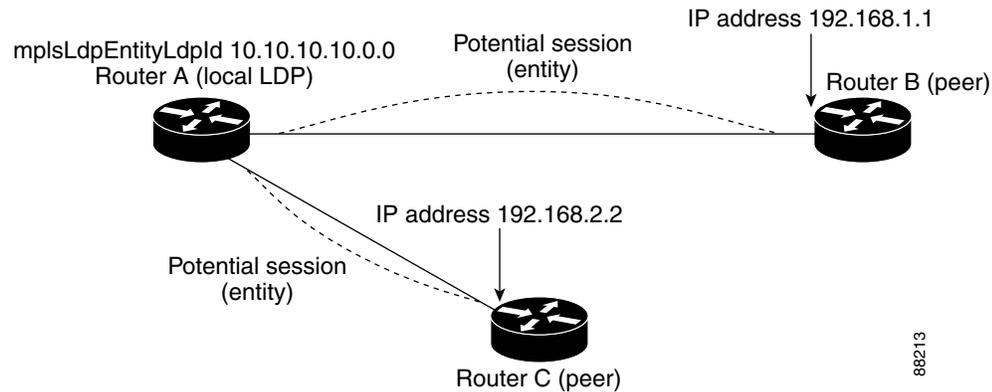
LDP operations related to an MPLS LDP MIB involve the following functional elements:

- LDP entity—Relates to an instance of LDP for purposes of exchanging label spaces; describes a potential session.
- LDP peer—Refers to a remote LDP entity (that is, a nonlocal LSR).
- LDP session—Refers to an active LDP process between a local LSR and a remote LDP peer.



In [Figure 2](#), Router A has potential sessions with two remote peers, Routers B and C. The `mplsLdpEntityLdpId` is 10.10.10.10.0.0, and the IP address of the peer active hello adjacency (`mplsLdpEntityIndex`) is 3232235777, which is the 32-bit representation of the IP address 192.168.1.1 for Router B.

**Figure 2** LDP Entity



## LDP Sessions and Peers

LDP sessions exist between local entities and remote peers for the purpose of distributing label spaces. There is always a one-to-one correspondence between an LDP peer and an LDP session. A single LDP session is an LDP instance that communicates across one or more network links with a single LDP peer.

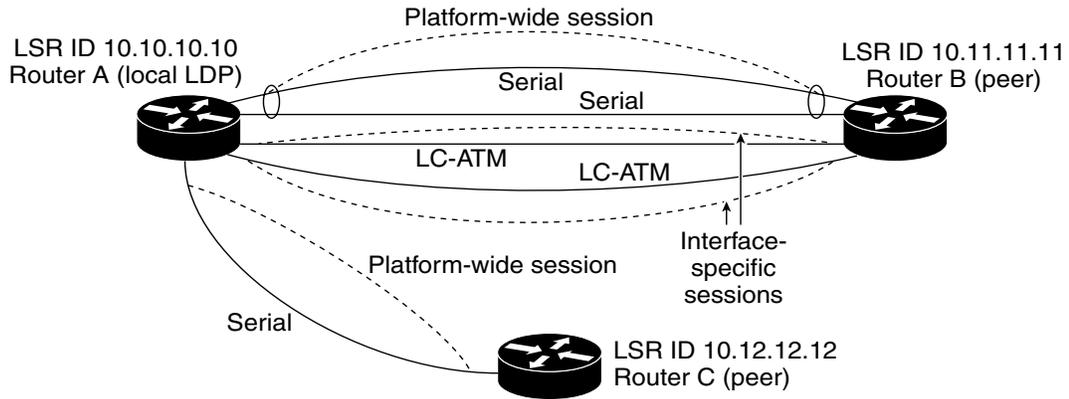
LDP supports the following types of sessions:

- **Interface-specific**—An interface-specific session uses interface resources for label space distributions. For example, each label-controlled ATM (LC-ATM) interface uses its own VPIs/VCIs for label space distributions. Depending on its configuration, an LDP platform can support zero, one, or more interface-specific sessions. Each LC-ATM interface has its own interface-specific label space and a nonzero label space ID.
- **Platform-wide**—An LDP platform supports a single platform-wide session for use by all interfaces that can share the same global label space. For Cisco platforms, all interface types except LC-ATM use the platform-wide session and have a label space ID of zero.

When a session is established between two peers, entries are created in the `mplsLdpPeerTable` and the `mplsLdpSessionTable` because they have the same indexing.

In [Figure 3](#), Router A has two remote peers, Routers B and C. Router A has a single platform-wide session that consists of two serial interfaces with Router B and another platform-wide session with Router C. Router A also has two interface-specific sessions with Router B.

**Figure 3 LDP Sessions**



88215

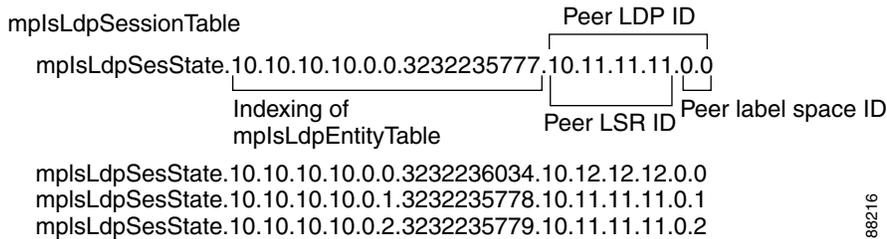
Figure 4 shows entries that correspond to the `mplsLdpPeerTable` and the `mplsLdpSessionTable` in Figure 3.

In Figure 4, `mplsLdpSesState` is a sample object from the `mplsLdpSessionTable` on Router A. There are four `mplsLdpSesState` sample objects shown (top to bottom). The first object represents a platform-wide session associated with two serial interfaces. The next two objects represent interface-specific sessions for the LC-ATM interfaces on Routers A and B. These interface-specific sessions have nonzero peer label space IDs. The last object represents a platform-wide session for the next peer, Router C.

The indexing is based on the entries in the `mplsLdpEntityTable`. It begins with the indexes of the `mplsLdpEntityTable` and adds the following:

- Peer LDP ID = 10.11.11.11.0.0  
The peer LDP ID consists of the peer LSR ID (four octets) and the peer label space ID (two octets).
- Peer LSR ID = 10.11.11.11
- Peer label space ID = 0.0  
The peer label space ID identifies a specific peer label space available within the LSR.

**Figure 4 Sample Indexing for an LDP Session**



88216

## LDP Hello Adjacencies

An LDP hello adjacency is a network link between a router and its peers. An LDP hello adjacency enables two adjacent peers to exchange label binding information.

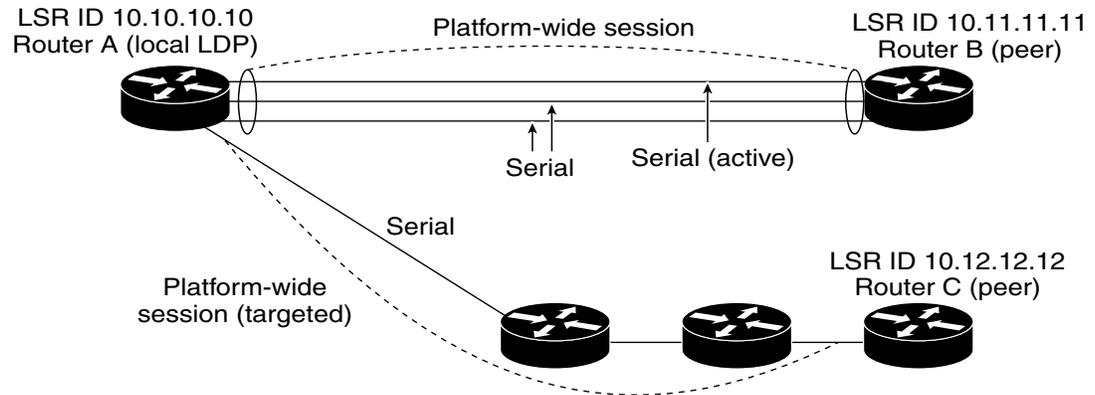
An LDP hello adjacency exists for each link on which LDP runs. Multiple LDP hello adjacencies exist whenever there is more than one link in a session between a router and its peer, such as in a platform-wide session.

A hello adjacency is considered active if it is currently engaged in a session, or nonactive if it is not currently engaged in a session.

A targeted hello adjacency is not directly connected to its peer and has an unlimited number of hops between itself and its peer. A linked hello adjacency is directly connected between two routers.

In [Figure 5](#), Router A has two remote peers, Routers B and C. Router A has a platform-wide session with Router B that consists of three serial interfaces, one of which is active and another platform-wide (targeted) session with Router C.

**Figure 5 Hello Adjacency**



88217

[Figure 6](#) shows entries in the `mplsLdpHelloAdjacencyTable`. There are four `mplsLdpHelloAdjHoldTime` sample objects (top to bottom). They represent the two platform-wide sessions and the four serial links shown in [Figure 5](#).

The indexing is based on the `mplsLdpSessionTable`. When the `mplsLdpHelloAdjIndex` enumerates the different links within a single session, the active link is `mplsLdpHelloAdjIndex = 1`.

**Figure 6 Sample Indexing for an LDP Hello Adjacency**

|                                          |                                                                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <code>mplsLdpHelloAdjacencyTable</code>  |                                                                                                                   |
| <code>mplsLdpHelloAdjHoldTimeRem.</code> | <code>10.10.10.10.0.0.3232235777.10.11.11.11.0.0.1</code>                                                         |
|                                          | Indexing of <code>mplsLdpSessionTable</code> <span style="float: right;"><code>mplsLdpHelloAdjIndex</code></span> |
| <code>mplsLdpHelloAdjHoldTimeRem.</code> | <code>10.10.10.10.0.0.3232235777.10.11.11.11.0.0.2</code>                                                         |
| <code>mplsLdpHelloAdjHoldTimeRem.</code> | <code>10.10.10.10.0.0.3232235777.10.11.11.11.0.0.3</code>                                                         |
| <code>mplsLdpHelloAdjHoldTimeRem.</code> | <code>10.10.10.10.0.0.3232236034.10.12.12.12.0.0.1</code>                                                         |

88218

## Events Generating MPLS LDP MIB Notifications in MPLS LDP MIB Version 8 Upgrade

When you enable MPLS LDP MIB notification functionality by issuing the `snmp-server enable traps mpls ldp` command, notification messages are generated and sent to a designated NMS in the network to signal the occurrence of specific events within Cisco IOS.

The MPLS LDP MIB objects involved in LDP status transitions and event notifications include the following:

- `mplsLdpSessionUp`—This message is generated when an LDP entity (a local LSR) establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).

- `mplsLdpSessionDown`—This message is generated when an LDP session between a local LSR and its adjacent LDP peer is terminated.
- `mplsLdpPathVectorLimitMismatch`—This message is generated when a local LSR establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.

The value of the path vector limit can range from 0 through 255; a value of 0 indicates that loop detection is off; any value other than zero up to 255 indicates that loop detection is on and, in addition, specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

We recommend that all LDP-enabled routers in the network be configured with the same path vector limit. Accordingly, the `mplsLdpPathVectorLimitMismatch` object exists in the MPLS LDP MIB to provide a warning message to the NMS when two routers engaged in LDP operations have different path vector limits.




---

**Note** This notification is generated only if the distribution method is downstream-on-demand.

---

- `mplsLdpFailedInitSessionThresholdExceeded`—This message is generated when a local LSR and an adjacent LDP peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts. The default number of attempts is 8. This default value is implemented and cannot be changed.

Eight failed attempts to establish an LDP session between a local LSR and an LDP peer, due to any type of incompatibility between the devices, causes this notification message to be generated. Cisco routers support the same features across multiple platforms.

Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges.

For example, if you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers try eight times to create an LDP session between themselves before the `mplsLdpFailedInitSessionThresholdExceeded` notification is generated and sent to the NMS as an informational message.

The LSRs whose label ranges do not overlap continue their attempt to create an LDP session between themselves after the eight-retry threshold is exceeded.

In such cases, the LDP threshold exceeded notification alerts the network administrator about a condition in the network that might warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers and/or other vendor LSRs in an MPLS network.

Among such incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI/VCI ranges (as noted above) or nonoverlapping Frame-Relay DLCI ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- Dissimilar types of LDP feature support

## MIB Tables in MPLS LDP MIB Version 8 Upgrade

Version 8 of the MPLS LDP MIB consists of the following tables:

- `mplsLdpEntityTable` (Table 1)—Contains entries for every active LDP hello adjacency. Nonactive hello adjacencies appear in the `mplsLdpHelloAdjacencyTable`, rather than this table. This table is indexed by the local LDP identifier for the interface and the IP address of the peer active hello adjacency. (See Figure 1.)

The advantage of showing the active hello adjacency instead of sessions in this table is that the active hello adjacency can exist even if an LDP session is not active (cannot be established). Previous implementations of the IETF MPLS-LDP MIB used sessions as the entries in this table. This approach was inadequate because as sessions went down, the entries in the entity table would disappear completely because the agent code could no longer access them. This resulted in the MIB failing to provide information about failed LDP sessions.

Directed adjacencies are also shown in this table. These entries, however, are always up administratively (`adminStatus`) and operationally (`operStatus`), because the adjacencies disappear if the directed session fails. Nondirected adjacencies might disappear from the MIB on some occasions, because adjacencies are deleted if the underlying interface becomes operationally down, for example.

- `mplsLdpEntityConfGenLRTable` (Table 2)—Contains entries for every LDP-enabled interface that is in the global label space. (For Cisco, this applies to all interfaces except LC-ATM. LC-ATM entities are shown in the `mplsLdpEntityConfAtmLRTable` instead.) Indexing is the same as it is for the `mplsLdpEntityTable`, except two indexes have been added, `mplsLdpEntityConfGenLRMin` and `mplsLdpEntityConfGenLRMax`. These additional indexes allow more than one label range to be defined. However, in the current Cisco IOS implementation, only one global label range is allowed.
- `mplsLdpEntityAtmParmsTable` (Table 3)—Contains entries for every LDP-enabled LC-ATM interface. This table is indexed the same as the `mplsLdpEntityTable` although only LC-ATM interfaces are shown.
- `mplsLdpEntityConfAtmLRTable` (Table 4)—Contains entries for every LDP-enabled LC-ATM interface. Indexing is the same as it is for the `mplsLdpEntityTable`, except two indexes have been added, `mplsLdpEntityConfAtmLRMinVpi` and `mplsLdpEntityConfAtmLRMinVci`. These additional indexes allow more than one label range to be defined. However, in the current Cisco IOS implementation, only one label range per LC-ATM interface is allowed.
- `mplsLdpEntityStatsTable` (Table 5)—Augments the `mplsLdpEntityTable` and shares the exact same indexing for performing GET and GETNEXT operations. This table shows additional statistics for entities.
- `mplsLdpPeerTable` (Table 6)—Contains entries for all peer sessions. This table is indexed by the local LDP identifier of the session, the IP address of the peer active hello adjacency, and the peer's LDP identifier. (See Figure 4.)
- `mplsLdpHelloAdjacencyTable` (Table 7)—Contains entries for all hello adjacencies. This table is indexed by the local LDP identifier of the associated session, the IP address of the peer active hello adjacency, the LDP identifier for the peer, and an arbitrary index that is set to the list position of the adjacency. (See Figure 6.)
- `mplsLdpSessionTable` (Table 8)—Augments the `mplsLdpPeerTable` and shares the same indexing for performing GET and GETNEXT operations. This table shows all sessions.
- `mplsLdpAtmSesTable` (Table 9)—Contains entries for LC-ATM sessions. Indexing is the same as it is for the `mplsLdpPeerTable`, except two indexes have been added, `mplsLdpSesAtmLRLowerBoundVpi` and `mplsLdpSesAtmLRLowerBoundVci`. These additional indexes allow more than one label range to be defined. However, in the current Cisco IOS implementation, only one label range per LC-ATM interface is allowed.

- `mplsLdpSesStatsTable` (Table 10)—Augments the `mplsLdpPeerTable` and shares the exact same indexing for performing GET and GETNEXT operations. This table shows additional statistics for sessions.

## mplsLdpEntityTable

Table 1 lists the `mplsLdpEntityTable` objects and their descriptions.

**Table 1** *mplsLdpEntityTable Objects and Descriptions*

| Object                                       | Description                                                                                                                                                                                                       |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>mplsLdpEntityEntry</code>              | Represents an LDP entity, which is a potential session between two peers.                                                                                                                                         |
| <code>mplsLdpEntityLdpId</code>              | The LDP identifier (not accessible) consists of the local LSR ID (four octets) and the label space ID (two octets).                                                                                               |
| <code>mplsLdpEntityIndex</code>              | A secondary index that identifies this row uniquely. It consists of the IP address of the peer active hello adjacency, which is the 32-bit representation of the IP address assigned to the LSR (not accessible). |
| <code>mplsLdpEntityProtocolVersion</code>    | The version number of the LDP protocol to be used in the session initialization message.                                                                                                                          |
| <code>mplsLdpEntityAdminStatus</code>        | The administrative status of this LDP entity is always up. If the hello adjacency fails, this entity disappears from the <code>mplsLdpEntityTable</code> .                                                        |
| <code>mplsLdpEntityOperStatus</code>         | The operational status of this LDP entity. Values are unknown(0), enabled(1), and disabled(2).                                                                                                                    |
| <code>mplsLdpEntityTcpDscPort</code>         | The TCP discovery port for LDP or TDP. The default value is 646 (LDP).                                                                                                                                            |
| <code>mplsLdpEntityUdpDscPort</code>         | The UDP discovery port for LDP or TDP. The default value is 646 (LDP).                                                                                                                                            |
| <code>mplsLdpEntityMaxPduLength</code>       | The maximum PDU length that is sent in the common session parameters of an initialization message.                                                                                                                |
| <code>mplsLdpEntityKeepAliveHoldTimer</code> | The two-octet value that is the proposed keepalive hold time for this LDP entity.                                                                                                                                 |
| <code>mplsLdpEntityHelloHoldTimer</code>     | The two-octet value that is the proposed hello hold time for this LDP entity.                                                                                                                                     |
| <code>mplsLdpEntityInitSesThreshold</code>   | The threshold for notification when this entity and its peer are engaged in an endless sequence of initialization messages.<br>The default value is 8 and cannot be changed by SNMP or CLI.                       |
| <code>mplsLdpEntityLabelDistMethod</code>    | The specified method of label distribution for any given LDP session. Values are downstreamOnDemand(1) and downstreamUnsolicited(2).                                                                              |
| <code>mplsLdpEntityLabelRetentionMode</code> | Can be configured to use either conservative(1) for LC-ATM or liberal(2) for all other interfaces.                                                                                                                |

**Table 1** *mplsLdpEntityTable Objects and Descriptions (continued)*

| <b>Object</b>                   | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpEntityPVLMisTrapEnable   | <p>Indicates whether the mplsLdpPVLMismatch trap should be generated.</p> <p>If the value is enabled(1), the trap is generated. If the value is disabled(2), the trap is not generated. The default is disabled(2).</p> <p><b>Note</b> The mplsLdpPVLMismatch trap is generated only if mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>                                                                                              |
| mplsLdpEntityPVL                | <p>If the value of this object is 0, loop detection for path vectors is disabled. Otherwise, if this object has a value greater than zero, loop detection for path vectors is enabled, and the path vector limit is this value.</p> <p><b>Note</b> The mplsLdpEntityPVL object is non-zero only if mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>                                                                                   |
| mplsLdpEntityHopCountLimit      | <p>If the value of this object is 0, loop detection using hop counters is disabled.</p> <p>If the value of this object is greater than 0, loop detection using hop counters is enabled, and this object specifies this entity's maximum allowable value for the hop count.</p> <p><b>Note</b> The mplsLdpEntityHopCountLimit object is non-zero only if mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>                              |
| mplsLdpEntityTargPeer           | <p>If this LDP entity uses a targeted adjacency, this object is set to true(1). The default value is false(2).</p>                                                                                                                                                                                                                                                                                                                              |
| mplsLdpEntityTargPeerAddrType   | <p>The type of the internetwork layer address used for the extended discovery. This object indicates how the value of mplsLdpEntityTargPeerAddr is to be interpreted.</p>                                                                                                                                                                                                                                                                       |
| mplsLdpEntityTargPeerAddr       | <p>The value of the internetwork layer address used for the targeted adjacency.</p>                                                                                                                                                                                                                                                                                                                                                             |
| mplsLdpEntityOptionalParameters | <p>Specifies the optional parameters for the LDP initialization message. If the value is generic(1), no optional parameters are sent in the LDP initialization message associated with this entity.</p> <p>LC-ATM uses atmParameters(2) to specify that a row in the mplsLdpEntityAtmParmsTable corresponds to this entry.</p> <p><b>Note</b> Frame Relay parameters are not supported.</p>                                                     |
| mplsLdpEntityDiscontinuityTime  | <p>The value of sysUpTime on the most recent occasion when one or more of this entity's counters suffered a discontinuity. The relevant counters are the specific instances of any Counter32 or Counter64 object contained in the mplsLdpEntityStatsTable that are associated with this entity. If no such discontinuities have occurred since the last reinitialization of the local management subsystem, this object contains a 0 value.</p> |

**Table 1** *mplsLdpEntityTable Objects and Descriptions (continued)*

| Object                 | Description                                                                            |
|------------------------|----------------------------------------------------------------------------------------|
| mplsLdpEntityStorType  | The storage type for this entry is a read-only implementation that is always volatile. |
| mplsLdpEntityRowStatus | This object is a read-only implementation that is always active.                       |

## mplsLdpEntityConfGenLRTable

Table 2 lists the mplsLdpEntityConfGenLRTable objects and their descriptions.

**Table 2** *mplsLdpEntityConfGenLRTable Objects and Descriptions*

| Object                           | Description                                                                                                                                                                                                                                                                                                |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpEntityConfGenLREntry      | A row in the LDP Entity Configurable Generic Label Range table. One entry in this table contains information on a single range of labels; the range is defined by an upper boundary (VPI/VCI pair) and a lower boundary (VPI/VCI pair).<br>The current implementation supports one label range per entity. |
| mplsLdpEntityConfGenLRMin        | The minimum label configured for this range (not accessible).                                                                                                                                                                                                                                              |
| mplsLdpEntityConfGenLRMax        | The maximum label configured for this range (not accessible).                                                                                                                                                                                                                                              |
| mplsLdpEntityConfGenIfIndxOrZero | This value represents the SNMP IF-MIB index for the platform-wide entity. If the active hello adjacency is targeted, the value is 0.                                                                                                                                                                       |
| mplsLdpEntityConfGenLRStorType   | The storage type for this entry is a read-only implementation that is always volatile.                                                                                                                                                                                                                     |
| mplsLdpEntityConfGenLRRowStatus  | This object is a read-only implementation that is always active.                                                                                                                                                                                                                                           |

## mplsLdpEntityAtmParamsTable

Table 3 lists the mplsLdpEntityAtmParamsTable objects and their descriptions.

**Table 3** *mplsLdpEntityAtmParamsTable Objects and Descriptions*

| Object                       | Description                                                                           |
|------------------------------|---------------------------------------------------------------------------------------|
| mplsLdpEntityAtmParamsEntry  | Represents the ATM parameters and ATM information for this LDP entity.                |
| mplsLdpEntityAtmIfIndxOrZero | This value represents the SNMP IF-MIB index for the interface-specific LC-ATM entity. |
| mplsLdpEntityAtmMergeCap     | Denotes the merge capability of this entity.                                          |

**Table 3** *mplsLdpEntityAtmParmsTable Objects and Descriptions (continued)*

| <b>Object</b>                    | <b>Description</b>                                                                                                                                                                                                                                               |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpEntityAtmLRComponents     | Number of label range components in the initialization message. This also represents the number of entries in the mplsLdpEntityConfAtmLRTable that correspond to this entry.                                                                                     |
| mplsLdpEntityAtmVcDirectionality | If the value of this object is bidirectional(0), a given VCI within a given VPI is used as a label for both directions independently of one another.<br><br>If the value of this object is unidirectional(1), a given VCI within a VPI designates one direction. |
| mplsLdpEntityAtmLsrConnectivity  | The peer LSR can be connected indirectly by means of an ATM VP, so that the VPI values can be different on the endpoints. For that reason, the label must be encoded entirely within the VCI field.<br><br>Values are direct(1), the default, and indirect(2).   |
| mplsLdpEntityDefaultControlVpi   | The default VPI value for the non-MPLS connection.                                                                                                                                                                                                               |
| mplsLdpEntityDefaultControlVci   | The default VCI value for the non-MPLS connection.                                                                                                                                                                                                               |
| mplsLdpEntityUnlabTrafVpi        | VPI value of the VCC supporting unlabeled traffic. This non-MPLS connection is used to carry unlabeled (IP) packets.                                                                                                                                             |
| mplsLdpEntityUnlabTrafVci        | VCI value of the VCC supporting unlabeled traffic. This non-MPLS connection is used to carry unlabeled (IP) packets.                                                                                                                                             |
| mplsLdpEntityAtmStorType         | The storage type for this entry is a read-only implementation that is always volatile.                                                                                                                                                                           |
| mplsLdpEntityAtmRowStatus        | This object is a read-only implementation that is always active.                                                                                                                                                                                                 |

## **mplsLdpEntityConfAtmLRTable**

Table 4 lists the mplsLdpEntityConfAtmLRTable objects and their descriptions.

**Table 4** *mplsLdpEntityConfAtmLRTable Objects and Descriptions*

| <b>Object</b>                | <b>Description</b>                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpEntityConfAtmLREntry  | A row in the LDP Entity Configurable ATM Label Range Table. One entry in this table contains information on a single range of labels; the range is defined by an upper boundary (VPI/VCI pair) and a lower boundary (VPI/VCI pair). This is the same data used in the initialization message. This label range should overlap the label range of the peer. |
| mplsLdpEntityConfAtmLRMinVpi | The minimum VPI number configured for this range (not accessible).                                                                                                                                                                                                                                                                                         |

**Table 4** *mplsLdpEntityConfAtmLRTable Objects and Descriptions (continued)*

| Object                          | Description                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------|
| mplsLdpEntityConfAtmLRMinVci    | The minimum VCI number configured for this range (not accessible).                     |
| mplsLdpEntityConfAtmLRMaxVpi    | The maximum VPI number configured for this range (not accessible).                     |
| mplsLdpEntityConfAtmLRMaxVci    | The maximum VCI number configured for this range (not accessible).                     |
| mplsLdpEntityConfAtmLRStorType  | The storage type for this entry is a read-only implementation that is always volatile. |
| mplsLdpEntityConfAtmLRRowStatus | This object is a read-only implementation that is always active.                       |

## mplsLdpEntityStatsTable

Table 5 lists the mplsLdpEntityStatsTable objects and their descriptions.

**Table 5** *mplsLdpEntityStatsTable Objects and Descriptions*

| Object                          | Description                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpEntityStatsEntry         | These entries augment the mplsLdpEntityTable by providing additional information for each entry.                                  |
| mplsLdpAttemptedSessions        | Not supported in this feature.                                                                                                    |
| mplsLdpSesRejectedNoHelloErrors | A count of the session rejected/no hello error notification messages sent or received by this LDP entity.                         |
| mplsLdpSesRejectedAdErrors      | A count of the session rejected/parameters advertisement mode error notification messages sent or received by this LDP entity.    |
| mplsLdpSesRejectedMaxPduErrors  | A count of the session rejected/parameters max PDU length error notification messages sent or received by this LDP entity.        |
| mplsLdpSesRejectedLRErrors      | A count of the session rejected/parameters label range notification messages sent or received by this LDP entity.                 |
| mplsLdpBadLdpIdentifierErrors   | A count of the number of bad LDP identifier fatal errors detected by the session associated with this LDP entity.                 |
| mplsLdpBadPduLengthErrors       | A count of the number of bad PDU length fatal errors detected by the session associated with this LDP entity.                     |
| mplsLdpBadMessageLengthErrors   | A count of the number of bad message length fatal errors detected by the session associated with this LDP entity.                 |
| mplsLdpBadTlvLengthErrors       | A count of the number of bad Type-Length-Value (TLV) length fatal errors detected by the session associated with this LDP entity. |
| mplsLdpMalformedTlvValueErrors  | A count of the number of malformed TLV value fatal errors detected by the session associated with this LDP entity.                |

**Table 5** *mplsLdpEntityStatsTable Objects and Descriptions (continued)*

| Object                         | Description                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| mplsLdpKeepAliveTimerExpErrors | A count of the number of session keepalive timer expired errors detected by the session associated with this LDP entity. |
| mplsLdpShutdownNotifReceived   | A count of the number of shutdown notifications received related to the session associated with this LDP entity.         |
| mplsLdpShutdownNotifSent       | A count of the number of shutdown notifications sent related to the session associated with this LDP entity.             |

## mplsLdpPeerTable

Table 6 lists the mplsLdpPeerTable objects and their descriptions.

**Table 6** *mplsLdpPeerTable Objects and Descriptions*

| Object                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpPeerEntry              | Information about a single peer that is related to a session (not accessible).<br><br><b>Note</b> This table is augmented by the mplsLdpSessionTable.                                                                                                                                                                                                                                                                                                                                                |
| mplsLdpPeerLdpId              | The LDP identifier of this LDP peer (not accessible) consists of the peer LSR ID (four octets) and the peer label space ID (two octets).                                                                                                                                                                                                                                                                                                                                                             |
| mplsLdpPeerLabelDistMethod    | For any given LDP session, the method of label distribution. Values are downstreamOnDemand(1) and downstreamUnsolicited(2).                                                                                                                                                                                                                                                                                                                                                                          |
| mplsLdpPeerLoopDetectionForPV | An indication of whether loop detection based on path vectors is disabled or enabled for this peer.<br><br>For downstream unsolicited distribution (mplsLdpPeerLabelDistMethod is downstreamUnsolicited(2)), this object always has a value of disabled(0) and loop detection is disabled.<br><br>For downstream-on-demand distribution (mplsLdpPeerLabelDistMethod is downstreamOnDemand(1)), this object has a value of enabled(1), provided that loop detection based on path vectors is enabled. |
| mplsLdpPeerPVL                | If the value of mplsLdpPeerLoopDetectionForPV for this entry is enabled(1), this object represents that path vector limit for this peer.<br><br>If the value of mplsLdpPeerLoopDetectionForPV for this entry is disabled(0), this value should be 0.                                                                                                                                                                                                                                                 |

## mplsLdpHelloAdjacencyTable

Table 7 lists the mplsLdpHelloAdjacencyTable objects and their descriptions.

**Table 7** *mplsLdpHelloAdjacencyTable Objects and Descriptions*

| Object                     | Description                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpHelloAdjacencyEntry | Each row represents a single LDP hello adjacency. An LDP session can have one or more hello adjacencies (not accessible).                                                    |
| mplsLdpHelloAdjIndex       | An identifier for this specific adjacency (not accessible). The active hello adjacency has mplsLdpHelloAdjIndex equal to 1.                                                  |
| mplsLdpHelloAdjHoldTimeRem | The time remaining for this hello adjacency. This interval changes when the next hello message, which corresponds to this hello adjacency, is received.                      |
| mplsLdpHelloAdjType        | This adjacency is the result of a link hello if the value of this object is link(1). Otherwise, this adjacency is a result of a targeted hello and its value is targeted(2). |

## mplsLdpSessionTable

Table 8 lists the mplsLdpSessionTable objects and their descriptions.

**Table 8** *mplsLdpSessionTable Objects and Descriptions*

| Object                         | Description                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpSessionEntry            | An entry in this table represents information on a single session between an LDP entity and an LDP peer. The information contained in a row is read-only. This table augments the mplsLdpPeerTable.                                                                                                                                   |
| mplsLdpSesState                | The current state of the session. All of the states are based on the LDP or TDP state machine for session negotiation behavior.<br><br>The states are as follows: <ul style="list-style-type: none"> <li>• nonexistent(1)</li> <li>• initialized(2)</li> <li>• openrec(3)</li> <li>• opensent(4)</li> <li>• operational(5)</li> </ul> |
| mplsLdpSesProtocolVersion      | The version of the LDP protocol which this session is using. This is the version of the LDP protocol that has been negotiated during session initialization.                                                                                                                                                                          |
| mplsLdpSesKeepAliveHoldTimeRem | The keepalive hold time remaining for this session.                                                                                                                                                                                                                                                                                   |

**Table 8** *mplsLdpSessionTable Objects and Descriptions (continued)*

| Object                      | Description                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpSesMaxPduLen         | The value of maximum allowable length for LDP PDUs for this session. This value could have been negotiated during the session initialization.                                                                                                                                                                                                                                                  |
| mplsLdpSesDiscontinuityTime | The value of sysUpTime on the most recent occasion when one or more of this session's counters suffered a discontinuity. The relevant counters are the specific instances of any Counter32 or Counter64 object contained in the mplsLdpSesStatsTable associated with this session.<br><br>The initial value of this object is the value of sysUpTime when the entry was created in this table. |

## mplsLdpAtmSesTable

Table 9 lists the mplsLdpAtmSesTable objects and their descriptions.

**Table 9** *mplsLdpAtmSesTable Objects and Descriptions*

| Objects                      | Description                                                                                                                                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpAtmSesEntry           | An entry in this table represents information on a single label range intersection between an LDP entity and an LDP peer (not accessible). |
| mplsLdpAtmSesLRLowerBoundVpi | The minimum VPI number for this range (not accessible).                                                                                    |
| mplsLdpAtmSesLRLowerBoundVci | The minimum VCI number for this range (not accessible).                                                                                    |
| mplsLdpAtmSesLRUpperBoundVpi | The maximum VPI number for this range (read-only).                                                                                         |
| mplsLdpAtmSesLRUpperBoundVci | The maximum VCI number for this range (read-only).                                                                                         |

## mplsLdpSesStatsTable

Table 10 lists the mplsLdpSesStatsTable objects and their descriptions.

**Table 10** *mplsLdpSesStatsTable Objects and Descriptions*

| Object                          | Description                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsLdpSesStatsEntry            | An entry in this table represents statistical information on a single session between an LDP entity and an LDP peer. This table augments the mplsLdpPeerTable. |
| mplsLdpSesStatsUnkMesTypeErrors | This object is the count of the number of unknown message type errors detected during this session.                                                            |
| mplsLdpSesStatsUnkTlvErrors     | This object is the count of the number of unknown TLV errors detected during this session.                                                                     |

## VPN Contexts in MPLS LDP MIB Version 8 Upgrade

Within an MPLS Border Gateway Protocol (BGP) 4 Virtual Private Network (VPN) environment, separate LDP processes can be created for each VPN. These processes and their associated data are called LDP contexts. Each context is independent from all others and contains data specific only to that context.

Cisco IOS Release 12.0(11)ST and later releases include the VPN Aware LDP MIB feature that allows the LDP MIB to get VPN context information. The feature adds support for different contexts for different MPLS VPNs. Users of the MIB can view MPLS LDP processes for a given MPLS VPN. The VPN Aware LDP MIB feature does not change the syntax of the IETF MPLS-LDP MIB. It changes the number and types of entries within the tables.

The IETF MPLS-LDP MIB can show information about only one context at a time. You can specify a context, either a global context or an MPLS VPN context, using an SNMP security name.

The following sections describe topics related to the VPN Aware LDP MIB feature:

- [SNMP Contexts, page 20](#)
- [VPN Aware LDP MIB Sessions, page 21](#)
- [VPN Aware LDP MIB Notifications, page 22](#)

## SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

VPN-aware SNMP requires that SNMP manager and agent entities operating in a VPN environment agree on mapping between the SNMP security name and the VPN name. This mapping is created by using different contexts for the SNMP data of different VPNs, which is accomplished through the configuration of the SNMP View-based Access Control Model MIB (SNMP-VACM-MIB). The SNMP-VACM-MIB is configured with views so that a user on a VPN with a security name is allowed access to the restricted object space within the context of only that VPN.

SNMP request messages undergo three phases of security and access control before a response message is sent back with the object values within a VPN context:

- The first security phase is authentication of the username. During this phase, the user is authorized for SNMP access.
- The second phase is access control. During this phase, the user is authorized for SNMP access to the group objects in the requested SNMP context.
- In the third phase, the user can access a particular instance of a table entry. With this third phase, complete retrieval can be based on the SNMP context name.

IP access lists can be configured and associated with SNMP community strings. This feature enables you to configure an association between VRF instances and SNMP community strings. When a VRF instance is associated with an SNMP community string, SNMP processes requests coming in for a particular community string only if they are received from the configured VRF. If the community string contained in the incoming packet does not have a VRF associated with it, it is processed only if it came in through a non-VRF interface.

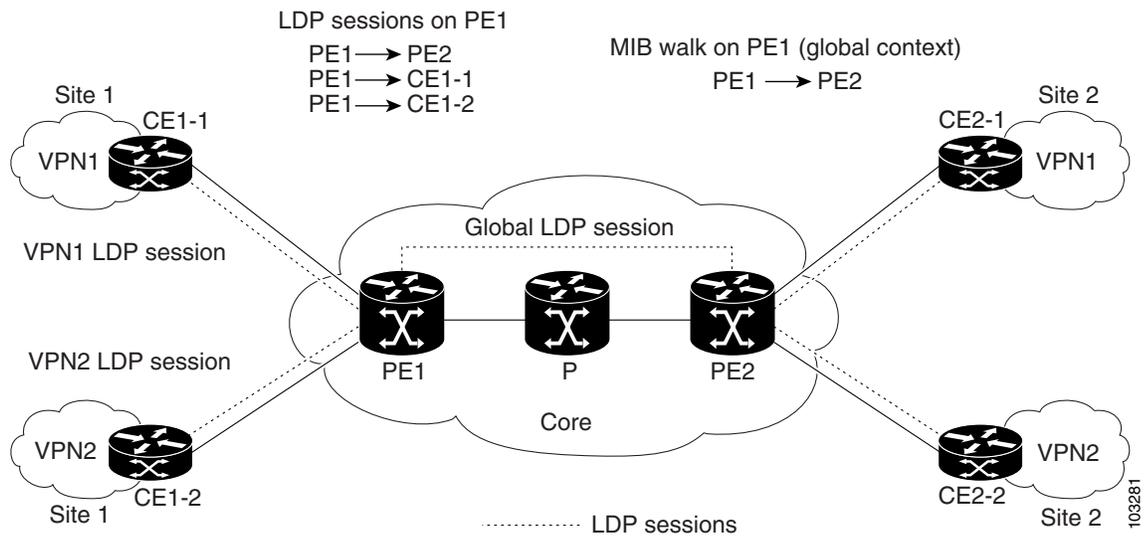
You can also enable or disable authentication traps for SNMP packets dropped due to VRF mismatches. By default, if SNMP authentication traps are enabled, VRF authentication traps are also enabled.

## VPN Aware LDP MIB Sessions

Prior to Cisco IOS Release 12.0(11)ST, an SNMP query to the MPLS LDP MIB returned information about global sessions only. A query did not return information about LDP sessions in a VPN context. The IETF MPLS LDP MIB retrieved information from global routing tables, but did not retrieve information from VPN routing and forwarding instances (VRFs) that store per-VPN routing data. The MPLS LDP MIB looked only at LDP processes in the global context and ignored all other sessions. A query on a VRF returned no information. You can view LDP processes in a VPN context.

Figure 7 shows a sample MPLS VPN network with the MPLS LDP sessions prior to the implementation of the VPN Aware LDP MIB feature.

**Figure 7 MPLS LDP Sessions Setup Before VPN Aware LDP MIB Feature**

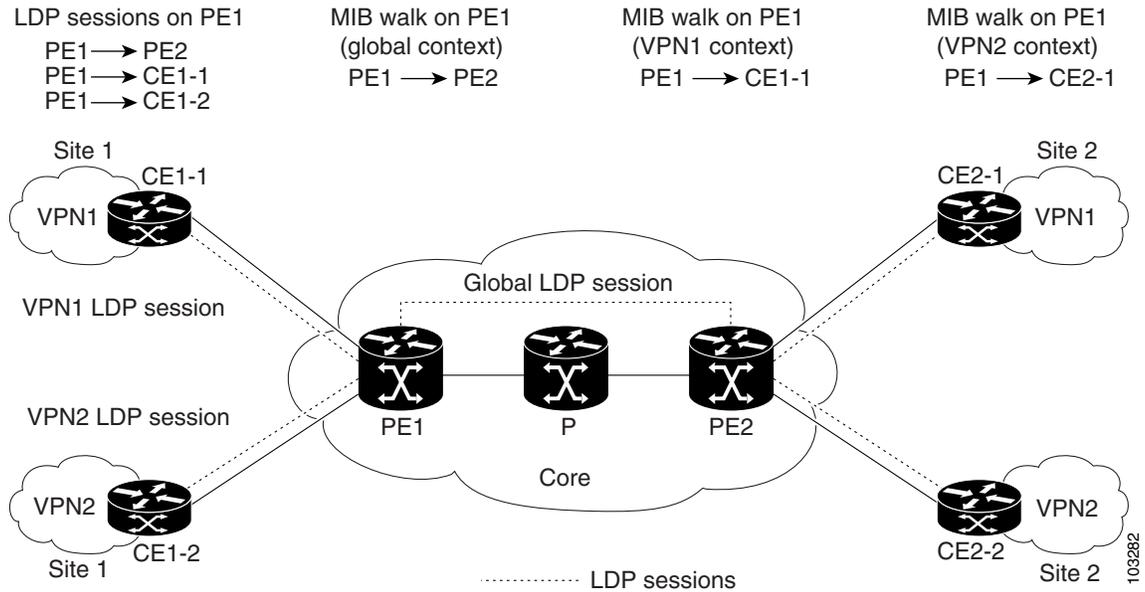


A MIB walk prior to this Cisco IOS release displayed only global session information.

With the VPN Aware LDP MIB enhancement in this Cisco IOS release, an SNMP query to the IETF MPLS-LDP-MIB supports both global and VPN contexts. This feature allows you to enter LDP queries on any VRF and on the core (global context). A query can differentiate between LDP sessions from different VPNs. LDP session information for a VPN stays in the context of that VPN. Therefore, the information from one VPN is not available to a user of a different VPN. The VPN Aware update to the LDP MIB also allows you to view LDP processes operating in a Carrier Supporting Carrier (CSC) network.

In an MPLS VPN, a service provider edge router (PE) might contain VRFs for several VPNs as well as a global routing table. To set up separate LDP processes for different VPNs on the same device, you need to configure each VPN with a unique securityName, contextName, and View-based Access Control Model (VACM) view. The VPN securityName must be configured for the IETF MPLS LDP MIB.

Figure 8 shows LDP sessions for a sample MPLS VPN network with the VPN Aware LDP MIB feature.

**Figure 8** MPLS LDP Sessions with the VPN Aware LDP MIB Feature

With the VPN Aware LDP MIB feature, you can do MIB queries or MIB walks for an MPLS VPN LDP session or a global LDP session.

**Note**

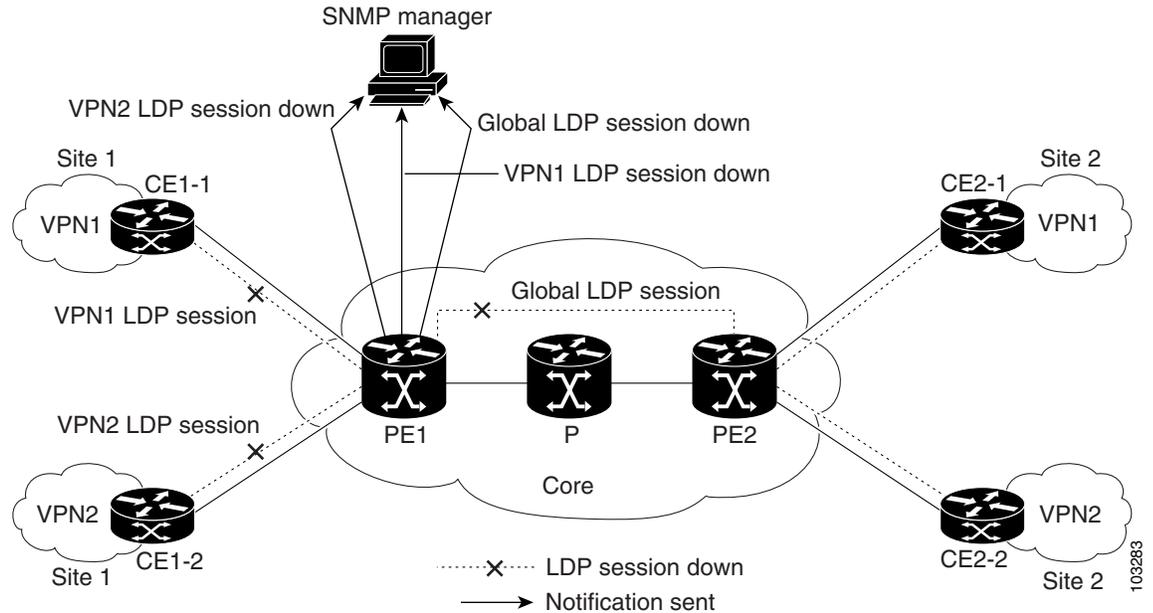
To verify LDP session information for a specific VPN, use the **show mpls ldp neighbor vrf *vpn-name* detail** command.

## VPN Aware LDP MIB Notifications

Prior to Cisco IOS Release 12.0(11)ST, all notification messages for MPLS LDP sessions were sent to the same designated network management station (NMS) in the network. The notifications were enabled with the **snmp-server enable traps mpls ldp** command.

Figure 9 shows LDP notifications that were sent before the implementation of the VPN Aware LDP MIB feature.

**Figure 9 LDP Notifications Sent Before the VPN Aware LDP MIB Feature**



The VPN Aware LDP MIB feature supports LDP notifications for multiple LDP contexts for VPNs. LDP notifications can be generated for the core (global context) and for different VPNs. You can cause notifications be sent to different NMS hosts for different LDP contexts. LDP notifications associated with a specific VRF are sent to the NMS designated for that VRF. LDP global notifications are sent to the NMS configured to receive global traps.

To enable LDP context notifications for the VPN Aware LDP MIB feature, use either the SNMP object `mplsLdpSessionsUpDownEnable` (in the global LDP context only) or the following extended global configuration commands.

To enable LDP notifications for the global context, use the following commands:

```
PE-Router(config)# snmp-server host host-address traps community mpls-ldp
```

```
PE-Router(config)# snmp-server enable traps mpls ldp
```

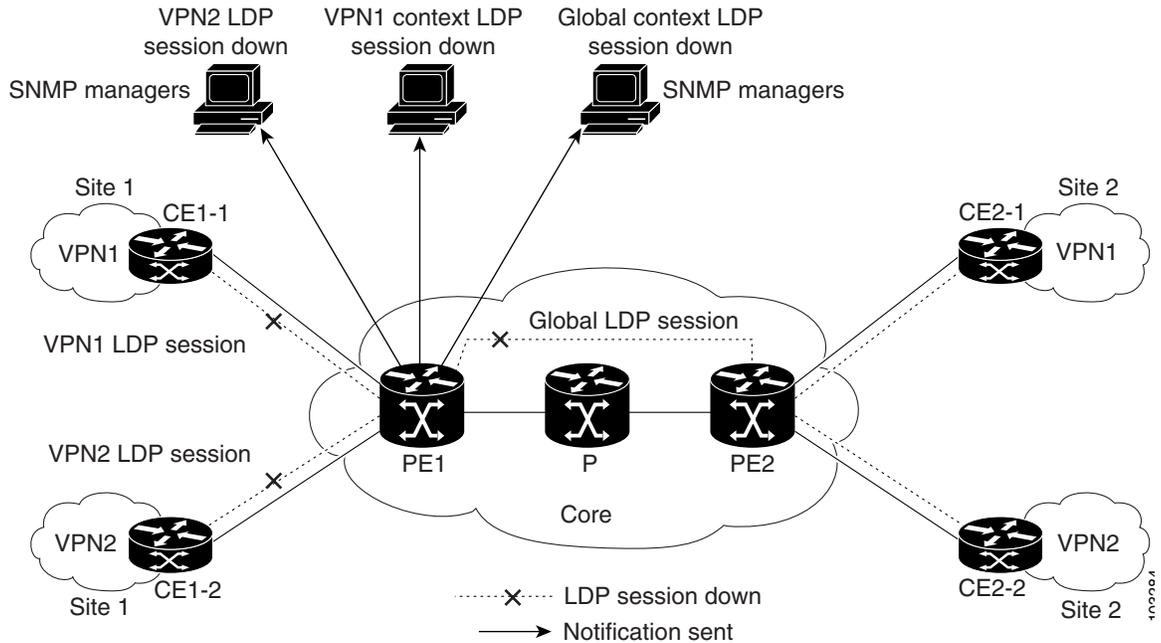
To enable LDP notifications for a VPN context, use the following commands:

```
PE-Router(config)# snmp-server host host-address vrf vrf-name version {v1|v2c|v3}
community community-string udp-port upd-port mpls-ldp
```

```
PE-Router(config)# snmp-server enable traps mpls ldp
```

Figure 10 shows LDP notifications with the VPN Aware LDP MIB feature.

**Figure 10** LDP Notifications With the VPN Aware LDP MIB Feature



## How to Configure MPLS LDP MIB Version 8 Upgrade

This section contains the following procedures:

- [Enabling the SNMP Agent, page 24](#) (required)
- [Enabling Cisco Express Forwarding, page 25](#) (required)
- [Enabling MPLS Globally, page 26](#) (required)
- [Enabling LDP Globally, page 27](#) (required)
- [Enabling MPLS on an Interface, page 28](#) (required)
- [Enabling LDP on an Interface, page 29](#) (required)
- [Configuring a VPN Aware LDP MIB, page 30](#) (required)
- [Verifying MPLS LDP MIB Version 8 Upgrade, page 36](#) (optional)

### Enabling the SNMP Agent

Perform this task to enable the SNMP agent.

#### SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community *string* [view *view-name*] [ro] [*number*]**

5. **end**
6. **write memory**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                    |
| Step 2 | <b>show running-config</b><br><br><b>Example:</b><br>Router# show running-config                                                                                                      | Displays the running configuration of the router so that you can determine if an SNMP agent is already running on the device.<br><br>If no SNMP information is displayed, continue with the next step.<br><br>If any SNMP information is displayed, you can modify the information or change it as desired.                                                                           |
| Step 3 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                     |
| Step 4 | <b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b> ] [ <i>number</i> ]<br><br><b>Example:</b><br>Router(config)# snmp-server community public ro | Configures read-only (ro) community strings for the MPLS LDP MIB. <ul style="list-style-type: none"> <li>• The <i>string</i> argument functions like a password, permitting access to SNMP functionality on label switch routers (LSRs) in an MPLS network.</li> <li>• The optional <b>ro</b> keyword configures read-only (ro) access to the objects in the MPLS LDP MIB.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                              | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                        |
| Step 6 | <b>write memory</b><br><br><b>Example:</b><br>Router# write memory                                                                                                                    | Writes the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.                                                                                                                                                                                                                                                                                |

## Enabling Cisco Express Forwarding

Perform this task to enable Cisco Express Forwarding or distributed Cisco Express Forwarding.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. `ip cef distributed`
4. `end`

## DETAILED STEPS

|        | Command or Action                                                                                         | Purpose                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                 | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>         | Enters global configuration mode.                                                                                   |
| Step 3 | <code>ip cef distributed</code><br><br><b>Example:</b><br>Router(config)# <code>ip cef distributed</code> | Enables distributed Cisco Express Forwarding.                                                                       |
| Step 4 | <code>end</code><br><br><b>Example:</b><br>Router(config)# <code>end</code>                               | Exits to privileged EXEC mode.                                                                                      |

## Enabling MPLS Globally

Perform this task to enable MPLS globally.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mpls ip`
4. `end`

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                       | <b>Purpose</b>                                                                        |
|---------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.               |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                     |
| <b>Step 3</b> | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip               | Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform. |
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                       | Exits to privileged EXEC mode.                                                        |

**Enabling LDP Globally**

Perform this task to enable LDP globally.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **mpls label protocol {ldp | tdp}**
4. **end**

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                       | <b>Purpose</b>                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>enable</code><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| <b>Step 2</b> | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal                           | Enters global configuration mode.                                                                                   |
| <b>Step 3</b> | <code>mpls label protocol {ldp   tdp}</code><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp | Specifies the platform default label distribution protocol.                                                         |
| <b>Step 4</b> | <code>end</code><br><br><b>Example:</b><br>Router(config)# end                                                 | Exits to privileged EXEC mode.                                                                                      |

**Enabling MPLS on an Interface**

Perform this task to enable MPLS on an interface.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface [type number]`
4. `mpls ip`
5. `end`

## DETAILED STEPS

|        | Command or Action                                                                                      | Purpose                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                 | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                         | Enters global configuration mode.                                                                                                                                  |
| Step 3 | <b>interface</b> [ <i>type number</i> ]<br><br><b>Example:</b><br>Router(config)# interface Ethernet 1 | Enters interface configuration mode.<br><ul style="list-style-type: none"><li>The <i>type number</i> argument identifies the interface to be configured.</li></ul> |
| Step 4 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                    | Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.                                                                    |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                            | Exits to privileged EXEC mode.                                                                                                                                     |

## Enabling LDP on an Interface

Perform this task to enable LDP on an interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **mpls label protocol** {*ldp* | *tdp* | *both*}
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                  | Purpose                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                     | Enters global configuration mode.                                                                                                                                  |
| Step 3 | <b>interface</b> [ <i>type number</i> ]<br><br><b>Example:</b><br>Router(config)# interface Ethernet 1             | Enters interface configuration mode.<br><ul style="list-style-type: none"><li>The <i>type number</i> argument identifies the interface to be configured.</li></ul> |
| Step 4 | <b>mpls label protocol</b> {ldp   tdp   both}<br><br><b>Example:</b><br>Router(config-if)# mpls label protocol ldp | Specifies the label distribution protocol to be used on a given interface.                                                                                         |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                        | Exits to privileged EXEC mode.                                                                                                                                     |

## Configuring a VPN Aware LDP MIB

To configure a VPN Aware LDP MIB, perform the following tasks:

- [Configuring SNMP Support for a VPN, page 30](#)
- [Configuring an SNMP Context for a VPN, page 31](#)
- [Associating an SNMP VPN Context with SNMPv1 or SNMPv2, page 33](#)

## Configuring SNMP Support for a VPN

Perform this task to configure SNMP support for a Virtual Private Network (VPN) or a remote VPN.

## SUMMARY STEPS

- enable**
- configure terminal**
- snmp-server host** *host-address* [**traps** | **informs**] [**version** {1 | 2c | 3 [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]
- snmp-server engineID remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*
- end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                                                                                    | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                        |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                                                                                                                                                                                                               | <p>Enters global configuration mode.</p>                                                                                                                                                                       |
| Step 3 | <p><b>snmp-server host</b> <i>host-address</i> [<b>traps</b>   <b>informs</b>]<br/>[<b>version</b> {<b>1</b>   <b>2c</b>   <b>3</b> [<b>auth</b>   <b>noauth</b>   <b>priv</b>]}]<br/><i>community-string</i> [<b>udp-port</b> <i>port</i>]<br/>[<i>notification-type</i>] [<b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b><br/>Router(config)# snmp-server host example.com<br/>vrf trap-vrf</p> | <p>Specifies the recipient of an SNMP notification operation and specifies the Virtual Private Network (VPN) routing and forwarding (VRF) instance table to be used for the sending of SNMP notifications.</p> |
| Step 4 | <p><b>snmp-server engineID remote</b> <i>ip-address</i><br/>[<b>udp-port</b> <i>udp-port-number</i>] [<b>vrf</b> <i>vrf-name</i>]<br/><i>engineid-string</i></p> <p><b>Example:</b><br/>Router(config)# snmp-server engineID remote<br/>172.16.20.3 vrf traps-vrf<br/>80000009030000B064EFE100</p>                                                                                                   | <p>Configures a name for the remote SNMP engine on a router.</p>                                                                                                                                               |
| Step 5 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config)# end</p>                                                                                                                                                                                                                                                                                                                                     | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                          |

## What to Do Next

Proceed to the [“Configuring an SNMP Context for a VPN”](#) section on page 31.

## Configuring an SNMP Context for a VPN

Perform this task to configure an SNMP context for a VPN. This sets up a unique SNMP context for a VPN, which allows you to access the VPN’s LDP session information.

## SNMP Context

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN’s specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

## VPN Route Distinguishers

A route distinguisher (RD) creates routing and forwarding tables for a VPN. Cisco IOS adds the RD to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

Either the RD is an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter an RD in either of these formats:

- 16-bit ASN: your 32-bit number, for example, 101:3.
- 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server context** *context-name*
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **context** *context-name*
7. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
8. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                  | Purpose                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                     | Enters global configuration mode.                                                                                         |
| Step 3 | <b>snmp-server context context-name</b><br><br><b>Example:</b><br>Router(config)# snmp-server context context1                                     | Creates and names an SNMP context.                                                                                        |
| Step 4 | <b>ip vrf vrf-name</b><br><br><b>Example:</b><br>Router(config)# ip vrf vrf1                                                                       | Configures a Virtual Private Network (VPN) routing and forwarding instance (VRF) table and enters VRF configuration mode. |
| Step 5 | <b>rd route-distinguisher</b><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:120                                                             | Creates a VPN route distinguisher.                                                                                        |
| Step 6 | <b>context context-name</b><br><br><b>Example:</b><br>Router(config-vrf)# context context1                                                         | Associates an SNMP context with a particular VRF.                                                                         |
| Step 7 | <b>route-target {import   export   both} route-target-ext-community</b><br><br><b>Example:</b><br>Router(config-vrf)# route-target export 100:1000 | (Optional) Creates a route-target extended community for a VRF.                                                           |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                           | Exits to privileged EXEC mode.                                                                                            |

## What to Do Next

Proceed to the [“Associating an SNMP VPN Context with SNMPv1 or SNMPv2”](#) section on page 33.

## Associating an SNMP VPN Context with SNMPv1 or SNMPv2

Perform this task to associate an SNMP VPN context with SNMPv1 or SNMPv2. This allows you to access LDP session information for a VPN using SNMPv1 or SNMPv2.

## SNMPv1 or SNMPv2 Security

SNMPv1 and SNMPv2 are not as secure as SNMPv3. SNMP Versions 1 and 2 use plain text communities and do not perform the authentication or security checks that SNMP Version 3 performs.

To configure the VPN Aware LDP MIB feature when using SNMP Version 1 or SNMP Version 2, you need to associate a community name with a VPN. This association causes SNMP to process requests coming in for a particular community string only if they come in from the configured VRF. If the community string contained in the incoming packet does not have an associated VRF, the packet is processed only if it came in through a non-VRF interface. This process prevents users outside the VPN from using a clear text community string to query the VPN data. However, this is not as secure as using SNMPv3.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user** *username group-name* [**remote host** [**udp-port port**]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access access-list**]
4. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context context-name**] [**read readview**] [**write writeview**] [**notify notifyview**] [**access access-list**]
5. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
6. **snmp-server enable traps** [*notification-type*]
7. **snmp-server host** *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] [*community-string*] [**udp-port port**] [**notification-type**] [**vrf vrf-name**]
8. **snmp mib community-map** *community-name* [**context context-name**] [**engineid engine-id**] [**security-name security-name**] **target-list vpn-list-name**
9. **snmp mib target list** *vpn-list-name* {**vrf vrf-name** | **host ip-address**}
10. **no snmp-server trap authentication vrf**
11. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                                                                                                                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                   |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                                                                                                                                                                                                                                                 | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                  |
| Step 3 | <p><b>snmp-server user</b> <i>username</i> <i>group-name</i> [<b>remote</b> <i>host</i> [<b>udp-port</b> <i>port</i>]] {<b>v1</b>   <b>v2c</b>   <b>v3</b> [<b>encrypted</b>] [<b>auth</b> {<b>md5</b>   <b>sha</b>} <i>auth-password</i>]} [<b>access</b> <i>access-list</i>]</p> <p><b>Example:</b><br/>Router(config)# snmp-server user customer1 group1 v1</p>                                                                     | <p>Configures a new user to an SNMP group.</p>                                                                                                                                                                                                                            |
| Step 4 | <p><b>snmp-server group</b> <i>group-name</i> {<b>v1</b>   <b>v2c</b>   <b>v3</b> {<b>auth</b>   <b>noauth</b>   <b>priv</b>}} [<b>context</b> <i>context-name</i>] [<b>read</b> <i>readview</i>] [<b>write</b> <i>writeview</i>] [<b>notify</b> <i>notifyview</i>] [<b>access</b> <i>access-list</i>]</p> <p><b>Example:</b><br/>Router(config)# snmp-server group group1 v1 context context1 read view1 write view1 notify view1</p> | <p>Configures a new SNMP group or a table that maps SNMP users to SNMP views.</p> <ul style="list-style-type: none"> <li>Use the <b>context</b> <i>context-name</i> keyword and argument to associate the specified SNMP group with a configured SNMP context.</li> </ul> |
| Step 5 | <p><b>snmp-server view</b> <i>view-name</i> <i>oid-tree</i> {<b>included</b>   <b>excluded</b>}</p> <p><b>Example:</b><br/>Router(config)# snmp-server view view1 ipForward included</p>                                                                                                                                                                                                                                               | <p>Creates or updates a view entry.</p>                                                                                                                                                                                                                                   |
| Step 6 | <p><b>snmp-server enable traps</b> [<i>notification-type</i>]</p> <p><b>Example:</b><br/>Router(config)# snmp-server enable traps</p>                                                                                                                                                                                                                                                                                                  | <p>Enables all SNMP notifications (traps or informs) available on your system.</p>                                                                                                                                                                                        |
| Step 7 | <p><b>snmp-server host</b> <i>host-address</i> [<b>traps</b>   <b>informs</b>] [<b>version</b> {<b>1</b>   <b>2c</b>   <b>3</b> [<b>auth</b>   <b>noauth</b>   <b>priv</b>]}] <i>community-string</i> [<b>udp-port</b> <i>port</i>] [<b>notification-type</b>] [<b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b><br/>Router(config)# snmp-server host 10.0.0.1 vrf customer1 public udp-port 7002</p>                                | <p>Specifies the recipient of an SNMP notification operation.</p>                                                                                                                                                                                                         |

|         | Command or Action                                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                            |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <pre>snmp mib community-map community-name [context context-name] [engineid engine-id] [security-name security-name] target-list vpn-list-name</pre> <p><b>Example:</b><br/>Router(config)# snmp mib community-maps<br/>community1 context context1 target-list<br/>commAVpn</p> | Associates an SNMP community with an SNMP context, Engine ID, or security name.                                                                                                                                                                                                                                    |
| Step 9  | <pre>snmp mib target list vpn-list-name {vrf vrf-name   host ip-address}</pre> <p><b>Example:</b><br/>Router(config)# snmp mib target list commAVpn<br/>vrf vrf1</p>                                                                                                             | Creates a list of target VRFs and hosts to associate with an SNMP community.                                                                                                                                                                                                                                       |
| Step 10 | <pre>no snmp-server trap authentication vrf</pre> <p><b>Example:</b><br/>Router(config)# no snmp-server trap<br/>authentication vrf</p>                                                                                                                                          | (Optional) Disables all SNMP authentication notifications (traps and informs) generated for packets received on VRF interfaces. <ul style="list-style-type: none"> <li>Use this command to disable authentication traps only for those packets on VRF interfaces with incorrect community associations.</li> </ul> |
| Step 11 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config) exit</p>                                                                                                                                                                                                                   | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                     |

## Verifying MPLS LDP MIB Version 8 Upgrade

Perform a MIB walk using your SNMP management tool to verify that the MPLS LDP MIB Version 8 Upgrade feature is functioning.

## Configuration Examples for MPLS LDP MIB Version 8 Upgrade

This section provides the following configuration examples:

- [MPLS LDP MIB Version 8 Upgrade Examples, page 36](#)
- [Configuring a VPN Aware SNMP Context for SNMPv1 or SNMPv2: Example, page 37](#)

## MPLS LDP MIB Version 8 Upgrade Examples

The following example shows how to enable an SNMP agent on the host NMS:

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# snmp-server community
```

The following example shows how to enable SNMPv1 and SNMPv2C on the host NMS. The configuration permits any SNMP agent to access all MPLS LDP MIB objects that have read-only permission using the community string public.

```
Router(config)# snmp-server community public
```

The following example shows how to allow read-only access to all MPLS LDP MIB objects relating to members of access list 4 that specify the comaccess community string. No other SNMP agents will have access to any of the MPLS LDP MIB objects.

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to enable LDP globally and then on an interface:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# mpls label protocol ldp
```

```
Router(config)# interface Ethernet1
```

```
Router(config-if)# mpls label protocol ldp
```

```
Router(config-if)# end
```

## Configuring a VPN Aware SNMP Context for SNMPv1 or SNMPv2: Example

The following configuration example shows how to configure a VPN Aware SNMP context for the MPLS LDP MIB Version 8 with SNMPv1 or SNMPv2:

```
snmp-server context A
snmp-server context B

ip vrf CustomerA
 rd 100:110
 context A
 route-target export 100:1000
 route-target import 100:1000
!

ip vrf CustomerB
 rd 100:120
 context B
 route-target export 100:2000
 route-target import 100:2000
!

interface Ethernet3/1
 description Belongs to VPN A
 ip vrf forwarding CustomerA
 ip address 10.0.0.0 255.255.0.0

interface Ethernet3/2
 description Belongs to VPN B
 ip vrf forwarding CustomerB
 ip address 10.0.0.1 255.255.0.0
```

```
snmp-server user commA grp1A v1
snmp-server user commA grp2A v2c
snmp-server user commB grp1B v1
snmp-server user commB grp2B v2c

snmp-server group grp1A v1 context A read viewA write viewA notify viewA
snmp-server group grp1B v1 context B read viewB write viewB notify viewB

snmp-server view viewA ipForward included
snmp-server view viewA ciscoPingMIB included
snmp-server view viewB ipForward included
snmp-server view viewB ciscoPingMIB included

snmp-server enable traps
snmp-server host 10.0.0.3 vrf CustomerA commA udp-port 7002
snmp-server host 10.0.0.4 vrf CustomerB commB udp-port 7002

snmp mib community-map commA context A target-list commAvpn
! Configures source address validation
snmp mib community-map commB context B target-list commBvpn
! Configures source address validation
snmp mib target list commAvpn vrf CustomerA
! Configures a list of VRFs or from which community commA is valid
snmp mib target list commBvpn vrf CustomerB
! Configures a list of VRFs or from which community commB is valid
```

## Additional References

The following sections provide references related to the MPLS LDP MIB Version 8 Upgrade feature.

## Related Documents

| Related Topic                                                                                                    | Document Title                                                                                                           |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| MPLS LDP configuration tasks                                                                                     | <a href="#">MPLS Label Distribution Protocol (LDP)</a>                                                                   |
| A description of SNMP agent support in Cisco IOS software for the MPLS Label Switching Router MIB (MPLS-LSR-MIB) | <a href="#">MPLS Label Switching Router MIB</a>                                                                          |
| A description of SNMP agent support in Cisco IOS software for the MPLS Traffic Engineering MIB (MPLS TE MIB)     | <a href="#">MPLS Traffic Engineering (TE) MIB</a>                                                                        |
| Configuration tasks for MPLS ATM network enhancements                                                            | <a href="#">MPLS Scalability Enhancements for the ATM LSR</a>                                                            |
| MPLS automatic bandwidth adjustment configuration tasks                                                          | <a href="#">MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels</a>                              |
| A description of MPLS differentiated types of service across an MPLS network                                     | <a href="#">MPLS Class of Service</a>                                                                                    |
| SNMP commands                                                                                                    | <a href="#">Cisco IOS Network Management Command Reference, Release 12.4T</a>                                            |
| SNMP configuration                                                                                               | “Configuring SNMP Support” chapter in the <a href="#">Cisco IOS Network Management Configuration Guide, Release 12.4</a> |
| SNMP support for VPNs                                                                                            | <a href="#">SNMP Notification Support for VPNs</a>                                                                       |
| SNMP context support for VPNs configuration tasks                                                                | <a href="#">SNMP Support over VPNs—Context Based Access Control</a>                                                      |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                                                                                                      | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>MPLS Label Distribution Protocol MIB (draft-ietf-mpls-ldp-mib-08.txt)</li> <li>SNMP-VACM-MIB<br/>The View-based Access Control Model (ACM) MIB for SNMP</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs                                                                                                                                                                                                                                                                                                                                        | Title                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| RFC 2233<br><br>The LDP implementation supporting the MPLS LDP MIB fully complies with the provisions of Section 10 of RFC 2026, which, in effect, states that the implementation of LDP is recommended for network devices that perform MPLS forwarding along normally routed paths, as determined by destination-based routing protocols. | <i>Interfaces MIB</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **context**
- **show mpls ldp neighbor**
- **snmp mib community-map**
- **snmp mib target list**
- **snmp-server community**
- **snmp-server context**
- **snmp-server enable traps (MPLS)**
- **snmp-server group**
- **snmp-server host**

- **snmp-server trap authentication vrf**

# Glossary

**ATM**—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

**downstream-on-demand distribution**—A label distribution method in which a downstream label switch router (LSR) sends a binding upstream only if the upstream LSR requests it.

**downstream unsolicited distribution**—A label distribution method in which labels are dispersed if a downstream label switch router (LSR) needs to establish a new binding with its neighboring upstream LSR. For example, an edge LSR might enable a new interface with another subnet. The LSR then announces to the upstream router a binding to reach this network.

**informs**—A type of notification message that is more reliable than a conventional trap notification message, because the informs message notification requires acknowledgment, but a trap notification does not.

**label**—A short, fixed-length data identifier that tells switching nodes how to forward data (packets or cells).

**label distribution**—The techniques and processes that are used by label switch routers (LSRs) to exchange label binding information for supporting hop-by-hop forwarding along normally routed paths.

**LDP**—Label Distribution Protocol. The protocol that supports MPLS hop-by-hop forwarding and the distribution of bindings between labels and network prefixes. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LSP**—label-switched path. A configured connection between two label switch routers (LSRs) in which label-switching techniques are used for packet forwarding; also a specific path through an MPLS network.

**LSR**—label switch router. A Multiprotocol Label Switching (MPLS) node that can forward native Layer 3 packets. The LSR forwards a packet based on the value of a label attached to the packet.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP). The value of a MIB object can be changed or retrieved by the use of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. A switching method for the forwarding of IP traffic through the use of a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**MPLS label distribution**—A constraint-based routing algorithm for routing label-switched path (LSP) tunnels.

**NMS**—network management station. A powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks. In the context of SNMP, an NMS is a device that performs SNMP queries to the SNMP agent of a managed device to retrieve or modify information.

**notification**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal to indicate that a significant network event has occurred. *See also* trap.

**RSVP**—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature of the packet streams they want to receive by specifying such items as bandwidth, jitter, and maximum burst.

**RTR**—Response Time Reporter. A tool that allows you to monitor network performance, network resources, and applications by measuring response times and availability.

**SNMP**—Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP enables a user to monitor and control network devices, manage configurations, collect statistics, monitor performance, and ensure network security.

**SNMP communities**—Authentication scheme that enables an intelligent network device to validate SNMP requests.

**SNMPv2c**—Version 2c of the Simple Network Management Protocol. SNMPv2c supports centralized as well as distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

**SNMPv3**—Version 3 of the Simple Network Management Protocol. Interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

**TDP**—Tag Distribution Protocol. A standard protocol used by MPLS-enabled routers to negotiate the tags (addresses) used for forwarding packets. *See also* LDP.

**TLV**—Type-Length-Value. A mechanism used by several routing protocols to carry a variety of attributes. Cisco Discovery Protocol (CDP), Label Discovery Protocol (LDP), and Border Gateway Protocol (BGP) are examples of protocols that use TLVs. BGP uses TLVs to carry attributes such as Network Layer Reachability Information (NLRI), Multiple Exit Discriminator (MED), and local preference.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant network event has occurred. Traps (notifications) are less reliable than inform requests, because the receiver of the trap does not send an acknowledgment of receipt; furthermore, the sender of the trap cannot determine if the trap was received. *See also* notification.

**VCC**—virtual channel connection. A logical circuit, made up of virtual channel links (VCLs), that carries data between two endpoints in an ATM network. Sometimes called a *virtual circuit connection*.

**VCI**—virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the virtual path identifier (VPI), is used to identify the next network virtual channel link (VCL) as the cell passes through a series of ATM switches on its way to its final destination.

**VCL**—virtual channel link. The logical connection that exists between two adjacent switches in an ATM network.

**VPI**—virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the virtual channel identifier (VCI), is used to identify the next network virtual channel link (VCL) as the cell passes through a series of ATM switches on its way to its final destination.

**VPN**—Virtual Private Network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF**—VPN routing and forwarding instance. A VRF 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 what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



## **MPLS Traffic Engineering**





# MPLS Traffic Engineering—DiffServ Aware (DS-TE)

---

This guide presents extensions made to Multiprotocol Label Switching Traffic Engineering (MPLS TE) that make it DiffServ aware. Specifically, the bandwidth reservable on each link for constraint-based routing (CBR) purposes can now be managed through at least two bandwidth pools: a *global pool* (also called BC0) and a *sub-pool* (also called BC1). The sub-pool can be limited to a smaller portion of the link bandwidth. Tunnels using the sub-pool bandwidth can then be used in conjunction with MPLS Quality of Service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network.

Beginning with Cisco IOS Release 12.2(33)SRB, DS-TE has been augmented to conform to IETF standards that were developed after the initial creation of Cisco DS-TE. Now both the traditional and the IETF versions of DS-TE can be run on your network; the new releases are backwards compatible.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

## Feature History

| Release       | Modification                                                                                                                                                                                 |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(11) ST   | DS-TE feature introduced.                                                                                                                                                                    |
| 12.0(14) ST   | Support was added for Cisco Series 7500(VIP) platform.<br>Support was added for IS-IS Interior Gateway Protocol.                                                                             |
| 12.0(14) ST-1 | Support was added for guaranteed bandwidth service directed to many destination prefixes (for example, guaranteed bandwidth service destined to an autonomous system or to a BGP community). |
| 12.0(22)S     | Feature was implemented in Cisco IOS Release 12.0(22)S.                                                                                                                                      |
| 12.2(14)S     | Feature was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                                     |
| 12.2(18)S     | Feature was implemented in Cisco IOS Release 12.2(18)S.                                                                                                                                      |
| 12.2(18)SXD   | Feature was implemented in Cisco IOS Release 12.2(18)SXD.                                                                                                                                    |
| 12.2(28)SB    | Feature was implemented in Cisco IOS Release 12.2(28)SB.                                                                                                                                     |
| 12.2(33)SRB   | Feature was augmented to include the new IETF-Standard functionality of DS-TE, as described in RFCs 3270, 4124, 4125, and 4127.                                                              |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

The guide contains the following sections:

- [Background and Overview, page 2](#)
- [Supported Standards, page 5](#)
- [Prerequisites, page 6](#)
- [Configuration Tasks, page 6](#)
- [Configuration Examples, page 13](#)
- [Command Reference, page 40](#)
- [Glossary, page 41](#)

## Background and Overview

MPLS traffic engineering allows constraint-based routing (CBR) of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. DiffServ-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of “guaranteed” traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a *sub-pool*, while the regular TE tunnel bandwidth is called the *global pool*. (The sub-pool is a portion of the global pool. In the new IETF-Standard, the global pool is called BC0 and the sub-pool is called BC1. These are two of an

eventually available eight Class Types). This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance in terms of delay, jitter, or loss for the guaranteed traffic.

For example, DS-TE can be used to ensure that traffic is routed over the network so that, on every link, there is never more than 40 per cent (or any assigned percentage) of the link capacity of guaranteed traffic (for example, voice), while there can be up to 100 per cent of the link capacity of regular traffic. Assuming that QoS mechanisms are also used on every link to queue guaranteed traffic separately from regular traffic, it then becomes possible to enforce separate “overbooking” ratios for guaranteed and regular traffic. In fact, for the guaranteed traffic it becomes possible to enforce no overbooking at all—or even an underbooking—so that very high QoS can be achieved end-to-end for that traffic, even while for the regular traffic a significant overbooking continues to be enforced.

Also, through the ability to enforce a maximum percentage of guaranteed traffic on any link, the network administrator can directly control the end-to-end QoS performance parameters without having to rely on over-engineering or on expected shortest path routing behavior. This is essential for transport of applications that have very high QoS requirements such as real-time voice, virtual IP leased line, and bandwidth trading, where over-engineering cannot be assumed everywhere in the network.

The new IETF-Standard functionality of DS-TE expands the means for allocating constrained bandwidth into two distinct models, called the “Russian Dolls Model” and the “Maximum Allocation Model”. They differ from each other as follows:

**Table 1** *Bandwidth Constraint Model Capabilities*

| MODEL                     | Achieves Bandwidth Efficiency | Ensures Isolation across Class Types |                         | Protects against QoS Degradation... |                             |
|---------------------------|-------------------------------|--------------------------------------|-------------------------|-------------------------------------|-----------------------------|
|                           |                               | When Preemption is Not Used          | When Preemption is Used | ...of the Premium Class Type        | ...of all other Class Types |
| <b>Maximum Allocation</b> | Yes                           | Yes                                  | Yes                     | Yes                                 | No                          |
| <b>Russian Dolls</b>      | Yes                           | No                                   | Yes                     | Yes                                 | Yes                         |

Therefore in practice, a Network Administrator might prefer to use:

- the Maximum Allocation Model when s/he needs to ensure isolation across all Class Types without having to use pre-emption, and s/he can afford to risk some QoS degradation of Class Types other than the Premium Class.
- the Russian Dolls Model when s/he needs to prevent QoS degradation of all Class Types and can impose pre-emption.

DS-TE involves extending OSPF (Open Shortest Path First routing protocol), so that the available sub-pool or class-type bandwidth at each preemption level is advertised in addition to the available global pool bandwidth at each preemption level. And DS-TE modifies constraint-based routing to take this more complex advertised information into account during path computation.

With the addition of IETF-Standard functionality (beginning with Cisco IOS Release 12.2(33)SRB), networks may accomplish DS-TE in three different combinations or “modes”, so that they may transition to the IETF-Standard formats in a manner that will not degrade their ongoing traffic service. These three situations or modes are summarized as follows:

1. **The original, or “Traditional” (pre-IETF-Standard) mode.** This describes networks that already operate the form of DS-TE that was introduced by Cisco a few years ago. Such networks can continue to operate in this traditional mode, even when they use the new Release 12.2(33)SRB and subsequent releases.
2. **The “Migration” or combination mode.** Networks already running traditional DS-TE that would like to upgrade to the IETF-Standard should first configure their routers into the Migration mode. This will allow them to continue to operate DS-TE without tunnels being torn down. In Migration mode, routers will continue to generate IGP and tunnel signalling as in the Traditional form, but now these routers will add TE-class mapping and will accept advertisement in both the Traditional and the new IETF-Standard formats.
3. **The “Liberal IETF” mode.** Networks already running in the Migration mode can then move into IETF formats by reconfiguring their routers into this flexible (hence “Liberal”) combination: their routers will henceforth generate IGP advertisement and tunnel signalling according to the new IETF Standard, but they will remain capable of accepting advertisement in the Traditional format, as well as in the new IETF format.

Table 2 summarizes these distinctions among the three modes.

**Table 2** Summary of DS-TE Mode behaviors

| MODE                | Uses<br>TE-class<br>mapping | Generates            |                       | Processes                |                       |
|---------------------|-----------------------------|----------------------|-----------------------|--------------------------|-----------------------|
|                     |                             | IGP<br>Advertisement | RSVP-TE<br>Signalling | IGP<br>Advertisement     | RSVP-TE<br>Signalling |
| <b>Traditional</b>  | No                          | traditional          | traditional           | traditional <sup>1</sup> | traditional           |
| <b>Migration</b>    | Yes                         | traditional          | traditional           | traditional &<br>IETF    | traditional &<br>IETF |
| <b>Liberal IETF</b> | Yes                         | IETF                 | traditional &<br>IETF | traditional &<br>IETF    | traditional &<br>IETF |

<sup>1</sup>Note that it is not possible for the Traditional mode to be liberal in what it accepts in terms of IGP, since it does not use TE-Class mapping and therefore cannot interpret the “Unreserved Bandwidth” in the IETF-compliant way when the Subpool Sub-TLV is absent.

## Benefits

DiffServ-aware Traffic Engineering enables service providers to perform separate admission control and separate route computation for discrete subsets of traffic (for example, voice and data traffic).

Therefore, by combining DS-TE with other IOS features such as QoS, the service provider can:

- Develop QoS services for end customers based on *signaled* rather than *provisioned* QoS
- Build the higher-revenue generating “strict-commitment” QoS services, without over-provisioning

- Offer virtual IP leased-line, Layer 2 service emulation, and point-to-point guaranteed bandwidth services including voice-trunking
- Enjoy the scalability properties offered by MPLS.

## Related Features and Technologies

The DS-TE feature is related to OSPF, IS-IS, RSVP (Resource reSerVation Protocol), QoS, and MPLS traffic engineering. Cisco documentation for all of these features is listed in the next section.

## Related Documents

For OSPF:

- [“Configuring OSPF”](#) in Cisco IOS *IP Routing Protocols Configuration Guide*, Release 12.4
- [“OSPF Commands”](#) in Cisco IOS *IP Routing Protocols Command Reference*, Release 12.4

For IS-IS:

- [“Configuring Integrated IS-IS”](#) in Cisco IOS *IP Routing Protocols Configuration Guide*, Release 12.4
- [“IS-IS Commands”](#) in Cisco IOS *IP Routing Protocols Command Reference*, Release 12.4

For RSVP:

- [“Configuring RSVP”](#) in “Part 5: Signalling” of Cisco IOS *Quality of Service Solutions Configuration Guide*, Release 12.4
- “ip rsvp . . .” commands in *Quality of Service Solutions Command Reference*, Release 12.4

For QoS:

- Cisco IOS *Quality of Service Solutions Configuration Guide*, Release 12.4
- Cisco IOS *Quality of Service Solutions Command Reference*, Release 12.4

For MPLS Traffic Engineering:

- [“Configuring MPLS Traffic Engineering”](#) within [“Configuring Multiprotocol Label Switching”](#) in Cisco IOS *Multiprotocol Label Switching Configuration Guide*, Release 12.4
- Cisco IOS *Multiprotocol Label Switching Command Reference*, Release 12.4

## Supported Standards

The traditional (pre-IETF Standard) version of DiffServ-aware MPLS Traffic Engineering conforms to the descriptions given in the following two documents:

- *Requirements for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, A. Chiu, W. Townsend, D. Skalecki & M. Tatham

- *Protocol Extensions for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, J. Boyle, K. Kompella, W. Townsend & D. Skalecki.

The IETF Standard for DiffServ-aware MPLS Traffic Engineering is described in the following four documents:

- [Multi-Protocol Label Switching \(MPLS\) Support of Differentiated Services](#) by F. Le Faucheur, L. Wu, B. Davie, P. Vaananen, R. Krishnan, P. Cheval, & J. Heinanen (RFC 3270)
- *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering* ed. by F. Le Faucheur (RFC 4124)
- *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering* ed. by F. Le Faucheur (RFC 4127)
- *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering* by F. Le Faucheur & W. Lai (RFC 4125).

The new concept of "Class-Type" defined in the IETF Standard corresponds to the prior concept of "bandwidth pool" that was implemented in the original version of DS-TE. Likewise, the two bandwidth pools implemented in the original version of DS-TE (global pool and sub-pool) correspond to two of the IETF Standard's new Class-Types (Class-Type 0 and Class-Type 1, respectively).

## Prerequisites

Your network must support the following Cisco IOS features in order to support guaranteed bandwidth services based on DiffServ-aware Traffic Engineering:

- MPLS
- IP Cisco Express Forwarding (CEF)
- OSPF or ISIS
- RSVP-TE
- QoS

## Configuration Tasks

This section presents the minimum set of commands you need to implement the DiffServ-aware Traffic Engineering feature—in other words, to establish a tunnel that reserves bandwidth to a sub-pool (renamed BC1 by the IETF-Standard).

The subsequent "[Configuration Examples](#)" section ([page 13](#)), presents these same commands in context and shows how, by combining them with QoS commands, you can build guaranteed bandwidth services.

## From Traditional to IETF-Standard Commands

DS-TE commands originally were developed from the then-existing command set that had been used to configure MPLS traffic engineering. The only difference introduced at that time to create DS-TE was the expansion of two commands:

- **ip rsvp bandwidth** was expanded to configure the size of the sub-pool on every link.
- **tunnel mpls traffic-eng bandwidth** was expanded to enable a TE tunnel to reserve bandwidth from the sub-pool.

## The ip rsvp bandwidth command

The early MPLS command had been

```
ip rsvp bandwidth x y
```

where  $x$  = the size of the only possible pool, and  $y$  = the size of a single traffic flow (ignored by traffic engineering).

Then, to create the original implementation of DS-TE, the command was made into

```
ip rsvp bandwidth x y sub-pool z
```

where  $x$  = the size of the global pool, and  $z$  = the size of the sub-pool.

With the addition of the IETF-Standard version of DS-TE, the command has been further extended to become:

```
ip rsvp bandwidth x y [[rdm x {subpool z | bc1 z}] | [mam bc0 x bc1 z]]
```

where  $x$  = the size of the global pool (now called **bc0**), and  $z$  = the size of the sub-pool (now called also **bc1**).

Two bandwidth constraint models also have become available, “Russian Dolls” (indicated by the keyword **rdm**) and “Maximum Allocation” (**mam**). The former model allows greater sharing of bandwidth across all Class Types (bandwidth pools), while the latter protects especially the premium Class Type. (The IETF Standard makes possible the future implementation of as many as seven sub-pools within one LSP, instead of just one sub-pool per LSP).

## The tunnel mpls traffic-eng bandwidth command

The pre-DS-TE traffic engineering command was

```
tunnel mpls traffic-eng bandwidth b
```

where  $b$  = the amount of bandwidth this tunnel requires.

So for the original DS-TE, you specified from which pool (global or sub) the tunnel's bandwidth would come. You could enter

```
tunnel mpls traffic-eng bandwidth sub-pool b
```

to indicate that the tunnel should use bandwidth from the sub-pool. Alternatively, you could enter

```
tunnel mpls traffic-eng bandwidth b
```

to indicate that the tunnel should use bandwidth from the global pool (which was the default).

With the addition of the IETF-Standard version of DS-TE, the command has been extended to become:

```
tunnel mpls traffic-eng bandwidth [sub-pool|class-type 1] b
```

where both **sub-pool** and **class-type 1** indicate the same, smaller bandwidth pool (now called class-type 1). The two keywords can be used interchangeably.

## The mpls traffic-eng ds-te commands

The IETF Standard introduces two new commands, one to indicate the Bandwidth Constraints model

```
mpls traffic-eng ds-te bc-model [rdm | mam]
```

and one to select the DS-TE mode:

```
mpls traffic-eng ds-te mode [migration|ietf]
```

(The concepts of bc-model and DS-TE mode were explained on [page 3](#)).

The first command allows you to select between the Russian Dolls Model (**rdm**) and the Maximum Allocation Model (**mam**) of bandwidth constraints.

The second command allows you to transition a network from traditional DS-TE tunnels to the IETF Standard without disrupting any of the tunnels' operation. To accomplish this, you first put the routers into Migration mode (using the **migration** keyword) and subsequently into the Liberal-IETF mode (using the **ietf** keyword).

## Transitioning a Network to the IETF Standard

Networks already operating DS-TE tunnels by means of the traditional, pre-IETF-Standard software can switch to the IETF-Standard without interrupting their DS-TE service by following this sequence:

1. Install Cisco IOS Release 12.2(33)SRB (or a subsequent release) on each router in the network, gradually, one router at a time, using Cisco's In Service Software Upgrade (ISSU) procedure which protects ongoing network traffic from interruption. (After that installation, DS-TE tunnels in the network will continue to operate by using the pre-IETF-Standard formats.)
2. Enter the global configuration command **mpls traffic-eng ds-te mode migration** on each router in the network, one router at a time. This will enable the routers to receive IETF-format IGP advertisement and RSVP-TE signaling, while the routers will continue to generate and receive the pre-Standard formats for those two functions.
3. After all the routers in the network have begun to operate in Migration mode, enter the global configuration command **mpls traffic-eng ds-te mode ietf** on each router, one at a time. This will cause the router to refresh its TE tunnels with IETF-compliant Path signaling, without disrupting the tunnels' operation. This mode also causes the router to generate IGP advertisement in the IETF-Standard format.

## Configuring DS-TE Tunnels

To establish a sub-pool (BC1) traffic engineering tunnel, you must enter configurations at three levels:

- the device level (router or switch router)
- the physical interface
- the tunnel interface

On the first two levels, you activate traffic engineering; on the third level—the tunnel interface—you establish the sub-pool tunnel. Therefore, it is only at the tunnel headend device that you need to configure all three levels. At the tunnel midpoints and tail, it is sufficient to configure the first two levels.

In the tables below, each command is explained in brief. For a more complete explanation of any command, type it into the Command Lookup Tool at <http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl>. (If prompted to log in there, use your Cisco.com account username and password).

### Level 1: Configuring the Device

At this level, you tell the device (router or switch router) to use accelerated packet-forwarding (known as Cisco Express Forwarding or CEF), MultiProtocol Label Switching (MPLS), traffic-engineering tunneling, a bandwidth constraints model, and either the OSPF or IS-IS routing algorithm (Open

Shortest Path First or Intermediate System to Intermediate System). This level is called the global configuration mode, because the configuration is applied globally, to the entire device, rather than to a specific interface or routing instance.

You enter the following commands:

|         | Command                                                                              | Purpose                                                                                                                                                                                                                                 |
|---------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | Router(config)# <b>ip cef distributed</b>                                            | Enables CEF—which accelerates the flow of packets through the device.                                                                                                                                                                   |
| Step 2  | Router(config)# <b>mpls traffic-eng tunnels</b>                                      | Enables MPLS, and specifically its traffic engineering tunnel capability.                                                                                                                                                               |
| Step 3  | Router(config)# <b>mpls traffic-eng ds-te bc-model [rdm   mam ]</b>                  | Specifies the bandwidth constraints model (see <a href="#">page 3</a> ).                                                                                                                                                                |
| Step 4  | Router(config)# <b>router ospf</b><br><br>[or]<br>Router(config)# <b>router isis</b> | Invokes the OSPF routing process for IP and puts the device into router configuration mode. Proceed now to Steps 10 and 11.<br><br>Alternatively, you may invoke the IS-IS routing process with this command, and continue with Step 5. |
| Step 5  | Router (config-router)# <b>net network-entity-title</b>                              | Specifies the IS-IS network entity title (NET) for the routing process.                                                                                                                                                                 |
| Step 6  | Router (config-router)# <b>metric-style wide</b>                                     | Enables the router to generate and accept IS-IS new-style TLVs (type, length, and value objects).                                                                                                                                       |
| Step 7  | Router (config-router)# <b>is-type level-n</b>                                       | Configures the router to learn about destinations inside its own area or “IS-IS level”.                                                                                                                                                 |
| Step 8  | Router (config-router)# <b>mpls traffic-eng level-n</b>                              | Specifies the IS-IS level (which must be same level as in the preceding step) to which the router will flood MPLS traffic-engineering link information.                                                                                 |
| Step 9  | Router (config-router)# <b>passive-interface loopback0</b>                           | Instructs IS-IS to advertise the IP address of the loopback interface without actually running IS-IS on that interface. Continue with Step 10 but don’t do Step 11—because Step 11 refers to OSPF.                                      |
| Step 10 | Router(config-router)# <b>mpls traffic-eng router-id loopback0</b>                   | Specifies that the traffic engineering router identifier is the IP address associated with the <i>loopback0</i> interface.                                                                                                              |
| Step 11 | Router(config-router)# <b>mpls traffic-eng area num</b>                              | Turns on MPLS traffic engineering for a particular OSPF area.                                                                                                                                                                           |

## Level 2: Configuring the Physical Interface

Having configured the device, you now must configure the interface on that device through which the tunnel will run. To do that, you first put the router into interface-configuration mode.

You then enable Resource Reservation Protocol (RSVP). This protocol is used to signal (set up) a traffic engineering tunnel, and to tell devices along the tunnel path to reserve a specific amount of bandwidth for the traffic that will flow through that tunnel. It is with this command that you establish the maximum size of the sub-pool (BC1).

Finally, you enable the MPLS traffic engineering tunnel feature on this physical interface—and if you will be relying on the IS-IS routing protocol, you enable that as well.

To accomplish these tasks, you enter the following commands:

|        | Command                                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <i>interface-id</i>                                                                                                                                                                                                                              | Moves configuration to the interface level, directing subsequent configuration commands to the specific interface identified by the <i>interface-id</i> .                                                                                                                                                                                             |
| Step 2 | Router(config-if)# <b>ip rsvp bandwidth</b> [ <i>interface-kbps</i> ] [ <i>single-flow-kbps</i> ] [[ <b>rdm</b> <i>kbps</i> ]{ <b>subpool</b> <i>kbps</i> }  <b>bc1</b> <i>subpool</i> }]  [ <b>max-reservable-bw</b> <i>kbps</i> <b>bc0</b> <i>kbps</i> <b>bc1</b> <i>kbps</i> ] | Enables RSVP on this interface, indicates the Bandwidth Constraints Model to be used (explained on <a href="#">page 3</a> ), and limits the amount of bandwidth RSVP can reserve on this interface. The sum of bandwidth used by all tunnels on this interface cannot exceed <i>interface-kbps</i> . (For more detail, see <a href="#">page 41</a> ). |
| Step 3 | Router(config-if)# <b>mpls traffic-eng tunnels</b>                                                                                                                                                                                                                                | Enables the MPLS traffic engineering tunnel feature on this interface.                                                                                                                                                                                                                                                                                |
| Step 4 | Router(config-if)# <b>ip router isis</b>                                                                                                                                                                                                                                          | Enables the IS-IS routing protocol on this interface. Do not enter this command if you are configuring for OSPF.                                                                                                                                                                                                                                      |

### Level 3: Configuring the Tunnel Interface

Now you create a set of attributes for the tunnel itself; those attributes are configured on the “tunnel interface” (not to be confused with the physical interface just configured above).

You enter the following commands:

|        | Command                                                                                                               | Purpose                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <b>tunnel1</b>                                                                       | Creates a tunnel interface (named in this example <b>tunnel1</b> ) and enters interface configuration mode.                                                                                                                                                    |
| Step 2 | Router(config-if)# <b>tunnel destination</b> <i>A.B.C.D</i>                                                           | Specifies the IP address of the tunnel tail device.                                                                                                                                                                                                            |
| Step 3 | Router(config-if)# <b>tunnel mode mpls traffic-eng</b>                                                                | Sets the tunnel’s encapsulation mode to MPLS traffic engineering.                                                                                                                                                                                              |
| Step 4 | Router(config-if)# <b>tunnel mpls traffic-eng bandwidth</b> { <b>sub-pool</b>   <b>class-type1</b> } <i>bandwidth</i> | Configures the tunnel’s bandwidth, and assigns it either to the sub-pool (when you use that keyword or the IETF-Standard keyword <b>class-type1</b> ) or to the global pool (when you leave out both keywords). For more detail, see <a href="#">page 49</a> . |
| Step 5 | Router(config-if)# <b>tunnel mpls traffic-eng priority</b>                                                            | Sets the priority to be used when the system determines which existing tunnels are eligible to be preempted.                                                                                                                                                   |
| Step 6 | Router(config-if)# <b>tunnel mpls traffic-eng path-option</b>                                                         | Configures the paths (hops) a tunnel should use. The user can enter an explicit path (can specify the IP addresses of the hops) or can specify a dynamic path (the router figures out the best set of hops).                                                   |

### Verifying the Configuration

To view the complete configuration you have entered, use the EXEC command **show running-config** and check its output display for correctness.

To check *just one tunnel*’s configuration, enter **show interfaces tunnel** followed by the tunnel interface number. And to see that tunnel’s RSVP bandwidth and flow, enter **show ip rsvp interface** followed by the name or number of the physical interface.

Here is an example of the information displayed by these latter two commands. (To see an explanation of each field used in the following displays, enter **show interfaces tunnel** or **show ip rsvp interface** into the Command Lookup Tool at <http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl>. If prompted to log in there, use your Cisco.com account username and password.)

```
Router#show interfaces tunnel 4
Tunnel4 is up, line protocol is down
 Hardware is Routing Tunnel
 MTU 1500 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
 Encapsulation TUNNEL, loopback not set, keepalive set (10 sec)
 Tunnel source 0.0.0.0, destination 0.0.0.0
 Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Output queue 0/0, 0 drops; input queue 0/75, 0 drops
 Five minute input rate 0 bits/sec, 0 packets/sec
 Five minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets, 0 restarts

Router#show ip rsvp interface pos4/0
interface allocated i/f max flow max sub max
PO4/0 300K 466500K 466500K 0M
```

To view *all tunnels at once* on the router you have configured, enter **show mpls traffic-eng tunnels brief**. The information displayed when tunnels are functioning properly looks like this:

```
Router#show mpls traffic-eng tunnels brief
Signalling Summary:
 LSP Tunnels Process: running
 RSVP Process: running
 Forwarding: enabled
 Periodic reoptimization: every 3600 seconds, next in 3029 seconds
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
GSR1_t0 192.168.1.13 - SR3/0 up/up
GSR1_t1 192.168.1.13 - SR3/0 up/up
GSR1_t2 192.168.1.13 - PO4/0 up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

When one or more tunnels is not functioning properly, the display could instead look like this. (In the following example, tunnels t0 and t1 are down, as indicated in the far right column).

```
Router#show mpls traffic-eng tunnels brief
Signalling Summary:
 LSP Tunnels Process: running
 RSVP Process: running
 Forwarding: enabled
 Periodic reoptimization: every 3600 seconds, next in 2279 seconds
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
GSR1_t0 192.168.1.13 - SR3/0 up/down
GSR1_t1 192.168.1.13 - SR3/0 up/down
GSR1_t2 192.168.1.13 - PO4/0 up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

To find out *why* a tunnel is down, insert its name into this same command, after adding the keyword **name** and omitting the keyword **brief**. For example:

```
Router#show mpls traffic-eng tunnels name GSR1_t0
Name:GSR1_t0 (Tunnel0) Destination:192.168.1.13
```

```
Status:
 Admin:up Oper:down Path: not valid Signalling:connected
```

If, as in this example, the Path is displayed as **not valid**, use the **show mpls traffic-eng topology** command to make sure the router has received the needed updates.

Additionally, you can use any of the following **show** commands to inspect particular aspects of the network, router, or interface concerned:

| To see information about... |                                                          |                                                                                             |
|-----------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------|
| this level                  | and this item...                                         | Use this command                                                                            |
| Network                     | Advertised bandwidth allocation information              | <b>show mpls traffic-eng link-management advertisements</b>                                 |
|                             | Preemptions along the tunnel path                        | <b>debug mpls traffic-eng link-management preemption</b>                                    |
|                             | Available TE link bandwidth on all head routers          | <b>show mpls traffic-eng topology</b> (described on <a href="#">page 41</a> )               |
| Router                      | Status of all tunnels currently signalled by this router | <b>show mpls traffic-eng link-management admission-control</b>                              |
|                             | Tunnels configured on midpoint routers                   | <b>show mpls traffic-eng link-management summary</b>                                        |
| Physical interface          | Detailed information on current bandwidth pools          | <b>show mpls traffic-eng link-management bandwidth-allocation</b> [ <i>interface-name</i> ] |
|                             | TE RSVP bookkeeping                                      | <b>show mpls traffic-eng link-management interfaces</b>                                     |
|                             | Entire configuration of one interface                    | <b>show run interface</b>                                                                   |

# Configuration Examples



## Note

The following 25 pages of examples illustrate DS-TE in the traditional, pre-IETF-Standard mode. You may update these examples simply by inserting the new Device Level command **mpls traffic-eng ds-te bc-model** as its proper use is shown in Step 3 on [page 9](#), and by applying the updated syntax within the two modified commands as each is shown respectively at the Physical Interface Level in Step 2 on [page 10](#) (**ip rsvp bandwidth**), and at the Tunnel Interface Level in Step 4 on [page 10](#) (**tunnel mpls traffic-eng bandwidth**).

First this section presents the DS-TE configurations needed to create the sub-pool tunnel. Then it presents the more comprehensive design for building end-to-end guaranteed bandwidth service, which involves configuring Quality of Service as well.

As shown in [Figure 1](#), the tunnel configuration involves at least three devices—tunnel head, midpoint, and tail. On each of those devices one or two network interfaces must be configured, for traffic ingress and egress.

**Figure 1**      **Sample Tunnel Topology**



## Tunnel Head

At the device level:

```
router-1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis
 router-1(config-router)# net
 49.0000.1000.0000.0010.00
 router-1(config-router)# metric-style wide
 router-1(config-router)# is-type level-1
|
router ospf 100
redistribute connected
network 10.1.1.0 0.0.0.255 area 0
 network 22.1.1.1 0.0.0.0 area
 0
```

```

router-1(config-router)# mpls traffic-eng level-1
router-1(config-router)# passive-interface Loopback0

```

[now one resumes the common command set]:

```

router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit

```

```

router-1(config)# interface Loopback0

```

At the virtual interface level:

```

router-1(config-if)# ip address 22.1.1.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit

```

At the device level:

```

router-1(config)# interface POS2/0/0

```

At the physical interface level (egress):

```

router-1(config-if)# ip address 10.1.1.1 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000
[and if using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

At the device level:

```

router-1(config)# interface Tunnel1

```

At the tunnel interface level:

```

router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 24.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
router-1(config-if)# exit
router-1(config)#

```

## Midpoint Devices

At the device level:

```

router-2# configure terminal
router-2(config)# ip cef distributed
router-2(config)# mpls traffic-eng tunnels

```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

```

router-2(config)# router isis
router-2(config-router)# net
49.0000.1000.0000.0012.00
router-2(config-router)# metric-style wide
router-2(config-router)# is-type level-1
router-2(config-router)# mpls traffic-eng
level-1
router-2(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit

```

```

router ospf 100
redistribute connected
network 11.1.1.0 0.0.0.255
area 0
network 12.1.1.0 0.0.0.255
area 0
network 25.1.1.1 0.0.0.0 area 0
mpls traffic-eng area 0

```

```

router-2(config)# interface Loopback0

```

At the virtual interface level:

```

router-2(config-if)# ip address 25.1.1.1 255.255.255.255
router-2(config-if)# no ip directed-broadcast
router-2(config-if)# exit

```

At the device level:

```

router-1(config)# interface POS4/0
router-1(config-if)# ip address 11.1.1.2 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000

```

[If using IS-IS instead of OSPF]:

```

router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

At the device level:

```

router-1(config)# interface POS4/1
router-1(config-if)# ip address 12.1.1.2 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000

```

[If using IS-IS instead of OSPF]:

```

router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

Note that there is no configuring of tunnel interfaces at the mid-point devices, only network interfaces and the device globally.

## Tail-End Device

At the device level:

```

router-3# configure terminal
router-3(config)# ip cef distributed

```

```
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                                                                                                                                                                                                                                                                           |                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-3(config)# router isis   router-3(config-router)# net   49.0000.1000.0000.0013.00   router-3(config-router)# metric-style wide   router-3(config-router)# is-type level-1    router-3(config-router)# mpls traffic-eng level-1   router-3(config-router)# passive-interface   Loopback0</pre> | <pre>router ospf 100  redistribute connected  network 12.1.1.0 0.0.0.255 area 0    network 24.1.1.1 0.0.0.0 area    0  mpls traffic-eng area 0</pre> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set]:

```
router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit
```

```
router-3(config)# interface Loopback0
```

At the virtual interface level:

```
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# no ip directed-broadcast
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

At the device level:

```
router-1(config)# interface POS4/0
 router-1(config-if)# ip address 12.1.1.3 255.255.255.0
 router-1(config-if)# mpls traffic-eng tunnels
 router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000
```

[If using IS-IS instead of OSPF]:

```
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

## Guaranteed Bandwidth Service Configuration

Having configured two bandwidth pools, you now can

- Use one pool, the sub-pool, for tunnels that carry traffic requiring strict bandwidth guarantees or delay guarantees
- Use the other pool, the global pool, for tunnels that carry traffic requiring only Differentiated Service.

Having a separate pool for traffic requiring strict guarantees allows you to limit the amount of such traffic admitted on any given link. Often, it is possible to achieve strict QoS guarantees only if the amount of guaranteed traffic is limited to a portion of the total link bandwidth.

Having a separate pool for other traffic (best-effort or diffserv traffic) allows you to have a separate limit for the amount of such traffic admitted on any given link. This is useful because it allows you to fill up links with best-effort/diffserv traffic, thereby achieving a greater utilization of those links.

## Providing Strict QoS Guarantees Using DS-TE Sub-pool Tunnels

A tunnel using sub-pool bandwidth can satisfy the stricter requirements if you do all of the following:

1. Select a queue—or in diffserv terminology, select a PHB (per-hop behavior)—to be used exclusively by the strict guarantee traffic. This shall be called the “GB queue.”

If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. On the Cisco 7500(VIP) it is the "priority" queue. You must configure the bandwidth of the queue to be at least equal to the bandwidth of the sub-pool.

If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used. On the Cisco 7500 (VIP) you use one of the existing Class-Based Weighted Fair Queuing (CBWFQ) queues.

2. Ensure that the guaranteed traffic sent through the sub-pool tunnel is placed in the GB queue *at the outbound interface of every tunnel hop*, and that no other traffic is placed in this queue.

You do this by marking the traffic that enters the tunnel with a unique value in the mpls exp bits field, and steering only traffic with that marking into the GB queue.

3. Ensure that this GB queue is never oversubscribed; that is, see that no more traffic is sent into the sub-pool tunnel than the GB queue can handle.

You do this by rate-limiting the guaranteed traffic before it enters the sub-pool tunnel. The aggregate rate of all traffic entering the sub-pool tunnel should be less than or equal to the bandwidth capacity of the sub-pool tunnel. Excess traffic can be dropped (in the case of delay/jitter guarantees) or can be marked differently for preferential discard (in the case of bandwidth guarantees).

4. Ensure that the amount of traffic entering the GB queue is limited to an appropriate percentage of the total bandwidth of the corresponding outbound link. The exact percentage to use depends on several factors that can contribute to accumulated delay in your network: your QoS performance objective, the total number of tunnel hops, the amount of link fan-in along the tunnel path, burstiness of the input traffic, and so on.

You do this by setting the sub-pool bandwidth of each outbound link to the appropriate percentage of the total link bandwidth (that is, by adjusting the z parameter of the **ip RSVP bandwidth** command).

## Providing Differentiated Service Using DS-TE Global Pool Tunnels

You can configure a tunnel using global pool bandwidth to carry best-effort as well as several other classes of traffic. Traffic from each class can receive differentiated service if you do all of the following:

1. Select a separate queue (a distinct diffserv PHB) for each traffic class. For example, if there are three classes (gold, silver, and bronze) there must be three queues (diffserv AF2, AF3, and AF4).
2. Mark each class of traffic using a unique value in the MPLS experimental bits field (for example gold = 4, silver = 5, bronze = 6).
3. Ensure that packets marked as Gold are placed in the gold queue, Silver in the silver queue, and so on. The tunnel bandwidth is set based on the expected aggregate traffic across all classes of service.

To control the amount of diffserv tunnel traffic you intend to support on a given link, adjust the size of the global pool on that link.

## Providing Strict Guarantees and Differentiated Service in the Same Network

Because DS-TE allows simultaneous constraint-based routing of sub-pool and global pool tunnels, strict guarantees and diffserv can be supported simultaneously in a given network.

## Guaranteed Bandwidth Service Examples

Given the many topologies in which Guaranteed Bandwidth Services can be applied, there is space here only to present two examples. They illustrate opposite ends of the spectrum of possibilities.

In the first example, the guaranteed bandwidth tunnel can be easily specified by its destination. So the forwarding criteria refer to a single destination prefix.

In the second example, there can be many final destinations for the guaranteed bandwidth traffic, including a dynamically changing number of destination prefixes. So the forwarding criteria are specified by Border Gateway Protocol (BGP) policies.

### Example with Single Destination Prefix

Figure 2 illustrates a topology for guaranteed bandwidth services whose destination is specified by a single prefix, either Site D (like a voice gateway, here bearing prefix 26.1.1.1) or a subnet (like the location of a web farm, here called “Province” and bearing prefix 26.1.1.0). Three services are offered:

- From Site A (defined as all traffic arriving at interface FE4/1/0): to host 26.1.1.1, 8 Mbps of guaranteed bandwidth with low loss, low delay and low jitter
- From Site B (defined as all traffic arriving at interface FE4/1/1): towards subnet 26.1.1.0, 32 Mbps of guaranteed bandwidth with low loss
- From Site C (defined as all traffic arriving at interface FE2/1/0): 30 Mbps of guaranteed bandwidth with low loss

**Figure 2** *Sample Topology for Guaranteed Bandwidth Services to a Single Destination Prefix*



These three services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the router-4 tail
- From the Head-2 router, 22.1.1.1, to the router-4 tail

Both tunnels use the same tail router, though they have different heads. (In [Figure 2](#) one midpoint router is shared by both tunnels. In the real world there could of course be many more midpoints.)

All POS interfaces in this example are OC3, whose capacity is 155 Mbps.

## Configuring Tunnel Head-1

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier in this Configuration Examples section). Then we present the QoS commands that guarantee end-to-end service on the subpool tunnel. (With the 7500 router, Modular QoS CLI is used.)

### Configuring the Pools and Tunnel

At the device level:

```

router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis
router-1(config-router)# net
49.0000.1000.0000.0010.00
router-1(config-router)# metric-style wide
router-1(config-router)# is-type level-1

router-1(config-router)# mpls traffic-eng
level-1
router-1(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:

router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
router ospf 100
redistribute connected

network 10.1.1.0 0.0.0.255 area 0
network 23.1.1.1 0.0.0.0 area
0
mpls traffic-eng area 0

```

Create a virtual interface:

```

router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit

```

At the outgoing physical interface:

```

router-1(config)# interface pos4/0
router-1(config-if)# ip address 10.1.1.1 255.0.0.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

At the tunnel interface:

```

router-1(config)# interface Tunnel1

```

```

router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic

```

To ensure that packets destined to host 26.1.1.1 and subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```

router-1(config)# ip route 26.1.1.0 255.255.255.0 Tunnel1
router-1(config)# exit

```

And in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```

router-1(config)# no tunnel mpls traffic-eng autoroute announce

```

### For Service from Site A to Site D

At the inbound physical interface (FE4/1/0):

1. In global configuration mode, create a class of traffic matching ACL 100, called "sla-1-class":

```

class-map match-all sla-1-class
 match access-group 100

```

2. Create an ACL 100 to refer to all packets destined to 26.1.1.1:

```

access-list 100 permit ip any host 26.1.1.1

```

3. Create a policy named "sla-1-input-policy", and according to that policy:

- a. Packets in the class called "sla-1-class" are rate-limited to:

- a rate of 8 million bits per second
- a normal burst of 1 million bytes
- a maximum burst of 2 million bytes

- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.
- c. Packets which exceed this rate are dropped.
- d. All other packets are marked with experimental bit 0 and are forwarded.

```

policy-map sla-1-input-policy
 class sla-1-class
 police 8000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
 exceed-action drop
 class class-default
 set-mpls-exp-transmit 0

```

4. The policy is applied to packets entering interface FE4/1/0.

```

interface FastEthernet4/1/0
 service-policy input sla-1-input-policy

```

### For Service from Site B to Subnet “Province”

At the inbound physical interface (FE4/1/1):

1. In global configuration mode, create a class of traffic matching ACL 120, called "sla-2-class":

```
class-map match-all sla-2-class
 match access-group 120
```

2. Create an ACL, 120, to refer to all packets destined to subnet 26.1.1.0:

```
access-list 120 permit ip any 26.1.1.0 0.0.0.255
```

3. Create a policy named “sla-2-input-policy”, and according to that policy:

- a. Packets in the class called “sla-2-class” are rate-limited to:

– a rate of 32 million bits per second

– a normal burst of 1 million bytes

– a maximum burst of 2 million bytes

- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

- c. Packets which exceed this rate are dropped.

- d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-2-input-policy
 class sla-2-class
 police 32000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
 exceed-action drop
 class class-default
 set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE4/1/1.

```
interface FastEthernet4/1/1
 service-policy input sla-2-input-policy
```

### For Both Services

The outbound interface (POS4/0) is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```
class-map match-all exp-5-traffic
 match mpls experimental 5
```

2. Create a policy named “output-interface-policy”. According to that policy, packets in the class “exp-5-traffic” are put in the priority queue (which is rate-limited to 62 kbits/sec).

```
policy-map output-interface-policy
 class exp-5-traffic
 priority 32
```

3. The policy is applied to packets exiting interface POS4/0.

```
interface POS4/0
 service-policy output output-interface-policy
```

The result of the above configuration lines is that packets entering the Head-1 router via interface FE4/1/0 destined to host 26.1.1.1, or entering the router via interface FE4/1/1 destined to subnet 26.1.1.0, will have their MPLS experimental bit set to 5. We assume that no other packets entering the

router (on any interface) are using this value. (If this cannot be assumed, an additional configuration must be added to mark all such packets to another experimental value.) Packets marked with experimental bit 5, when exiting the router via interface POS4/0, will be placed into the priority queue.

**Note**

Packets entering the router via FE4/1/0 or FE4/1/1 and exiting POS4/0 enter as IP packets and exit as MPLS packets.

## Configuring Tunnel Head-2

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier in this Configuration Examples section). Then we present the QoS commands that guarantee end-to-end service on the sub-pool tunnel.

### Configuring the Pools and Tunnel

At the device level:

```

router-2(config)# ip cef distributed
router-2(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# router isis router ospf 100
router-2(config-router)# net redistribute connected
49.0000.1000.0000.0011.00
router-2(config-router)# metric-style wide network 11.1.1.0 0.0.0.255 area 0
router-2(config-router)# is-type level-1 network 22.1.1.1 0.0.0.0 area
 0
router-2(config-router)# mpls traffic-eng mpls traffic-eng area 0
level-1
router-2(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit

```

Create a virtual interface:

```

router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# no ip directed broadcast
router-2(config-if)# exit

```

At the outgoing physical interface:

```

router-2(config)# interface pos0/0
router-2(config-if)# ip address 11.1.1.1 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-2(config-if)# ip router isis
[and in all cases]:
router-2(config-if)# exit

```

At the tunnel interface:

```

router-2(config)# interface Tunnel2

```

```

router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
router-2(config-if)# exit

```

And to ensure that packets destined to subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route, at the device level:

```

router-2(config)# ip route 26.1.1.0 255.255.255.0 Tunnel12
router-2(config)# exit

```

Finally, in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```

router-2(config)# no tunnel mpls traffic-eng autoroute announce

```

### For Service from Site C to Subnet "Province"

At the inbound physical interface (FE2/1/0):

1. In global configuration mode, create a class of traffic matching ACL 130, called "sla-3-class":

```

class-map match-all sla-3-class
 match access-group 130

```

2. Create an ACL, 130, to refer to all packets destined to subnet 26.1.1.0:

```

access-list 130 permit ip any 26.1.1.0 0.0.0.255

```

3. Create a policy named "sla-3-input-policy", and according to that policy:

- a. Packets in the class called "sla-3-class" are rate-limited to:

– a rate of 30 million bits per second

– a normal burst of 1 million bytes

– a maximum burst of 2 million bytes

- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

- c. Packets which exceed this rate are dropped.

- d. All other packets are marked with experimental bit 0 and are forwarded.

```

policy-map sla-3-input-policy
 class sla-3-class
 police 30000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
 exceed-action drop
 class class-default
 set-mpls-exp-transmit 0

```

4. The policy is applied to packets entering interface FE2/1/0.

```

interface FastEthernet2/1/0
 service-policy input sla-3-input-policy

```

The outbound interface POS0/0 is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```

class-map match-all exp-5-traffic

```

```
match mpls experimental 5
```

2. Create a policy named “output-interface-policy”. According to that policy, packets in the class “exp-5-traffic” are put in the priority queue (which is rate-limited to 32 kbits/sec).

```
policy-map output-interface-policy
 class exp-5-traffic
 priority 32
```

3. The policy is applied to packets exiting interface POS0/0:

```
interface POS0/0
 service-policy output output-interface-policy
```

As a result of all the above configuration lines, packets entering the Head-2 router via interface FE2/1/0 and destined for subnet 26.1.1.0 have their IP precedence field set to 5. It is assumed that no other packets entering this router (on any interface) are using this precedence. (If this cannot be assumed, an additional configuration must be added to mark all such packets with another precedence value.) When exiting this router via interface POS0/0, packets marked with precedence 5 are placed in the priority queue.

**Note**

Packets entering the router via FE2/1/0 and exiting through POS0/0 enter as IP packets and exit as MPLS packets.

## Tunnel Midpoint Configuration [Mid-1]

All four interfaces on the midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

### Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef distributed
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-3(config)# router isis router-3(config-router)# net 49.0000.2400.0000.0011.00 router-3(config-router)# metric-style wide router-3(config-router)# is-type level-1 router-3(config-router)# mpls traffic-eng level-1 router-3(config-router)# passive-interface Loopback0 router-3(config-router)# router-3(config-router)# [now one resumes the common command set]: router-3(config-router)# mpls traffic-eng router-id Loopback0 router-3(config-router)# exit</pre> | <pre>router ospf 100 redistribute connected network 10.1.1.0 0.0.0.255 area 0 network 11.1.1.0 0.0.0.255 area 0 network 24.1.1.1 0.0.0.0 area 0 network 12.1.1.0 0.0.0.255 area 0 network 13.1.1.0 0.0.0.255 area 0 mpls traffic-eng area 0</pre> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Create a virtual interface:

```

router-3(config)# interface Loopback0
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# exit

```

At the physical interface level (ingress):

```

router-3(config)# interface pos2/1
router-3(config-if)# ip address 10.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

```

router-3(config)# interface pos1/1
router-3(config-if)# ip address 11.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the physical interface level (egress):

```

router-3(config)# interface pos3/1
router-3(config-if)# ip address 12.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

```

router-3(config)# interface pos4/1
router-3(config-if)# ip address 13.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

## Tunnel Midpoint Configuration [Mid-2]

Both interfaces on the midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

### Configuring the Pools and Tunnel

At the device level:

```

router-5(config)# ip cef distributed
router-5(config)# mpls traffic-eng tunnels

```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

```

router-5(config)# router isis |router ospf 100
 |redistribute connected
router-5(config-router)# net
49.2500.1000.0000.0012.00

```

```

router-5(config-router)# metric-style wide
router-5(config-router)# is-type level-1

router-5(config-router)# mpls traffic-eng
level-1
router-5(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit

```

```

network 13.1.1.0 0.0.0.255 area 0
network 14.1.1.0 0.0.0.255
area 0
network 25.1.1.1 0.0.0.0 area
0
mpls traffic-eng area 0

```

Create a virtual interface:

```

router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit

```

At the physical interface level (ingress):

```

router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit

```

At the physical interface level (egress):

```

router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit

```

## Tunnel Tail Configuration

The inbound interfaces on the tail router are configured identically to the inbound interfaces of the midpoint routers (except, of course, for the ID of each particular interface):

### Configuring the Pools and Tunnels

At the device level:

```

router-4(config)# ip cef distributed
router-4(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

```

```

router-4(config)# router isis
router-4(config-router)# net
49.0000.2700.0000.0000.00
router-4(config-router)# metric-style wide

```

```

router ospf 100
redistribute connected
network 12.1.1.0 0.0.0.255 area 0

```

```

router-4(config-router)# is-type level-1
router-4(config-router)# mpls traffic-eng
level-1
router-4(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# exit

```

```

network 14.1.1.0 0.0.0.255
area 0
network 27.1.1.1 0.0.0.0 area
0
mpls traffic-eng area 0

```

Create a virtual interface:

```

router-4(config)# interface Loopback0
router-4(config-if)# ip address 27.1.1.1 255.255.255.255
router-4(config-if)# exit

```

At the physical interface (ingress):

```

router-4(config)# interface pos2/1
router-4(config-if)# ip address 12.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

router-4(config)# interface pos2/2
router-4(config-if)# ip address 14.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

```

Because the tunnel ends on the tail (does not include any outbound interfaces of the tail router), no outbound QoS configuration is used.

## Example with Many Destination Prefixes

Figure 3 illustrates a topology for guaranteed bandwidth services whose destinations are a set of prefixes. Those prefixes usually share some common properties such as belonging to the same Autonomous System (AS) or transiting through the same AS. Although the individual prefixes may change dynamically because of route flaps in the downstream autonomous systems, the properties the prefixes share will not change. Policies addressing the destination prefix set are enforced through Border Gateway Protocol (BGP), which is described in the following documents:

- “Configuring QoS Policy Propagation via Border Gateway Protocol” in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_c/qcprt1/qcdprop.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt1/qcdprop.htm))
- “Configuring BGP” in the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt2/1cdbgp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdbgp.htm))

- “BGP Commands” in the *Cisco IOS IP and IP Routing Command Reference*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_r/iprprt2/1rdbgp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/1rdbgp.htm))
- “BGP-Policy Command” in the *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_r/qrdcmd1.htm#xtocid89313](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/qrdcmd1.htm#xtocid89313))

In this example, three guaranteed bandwidth services are offered, each coming through a 7500 or a 12000 edge device:

- Traffic coming from Site A (defined as all traffic arriving at interface FE4/1/0) and from Site C (defined as all traffic arriving at interface FE2/1) destined to AS5
- Traffic coming from Sites A and C that transits AS5 but is not destined to AS5. (In the figure, the transiting traffic will go to AS6 and AS7)
- Traffic coming from Sites A and C destined to prefixes advertised with a particular BGP community attribute (100:1). In this example, Autonomous Systems #3, #5, and #8 are the BGP community assigned the attribute 100:1.

**Figure 3** *Sample Topology for Guaranteed Bandwidth Service to Many Destination Prefixes*



The applicability of guaranteed bandwidth service is not limited to the three types of multiple destination scenarios described above. There is not room in this document to present all possible scenarios. These three were chosen as representative of the wide range of possible deployments.

The guaranteed bandwidth services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the tail

- From the Head-2 router, 22.1.1.1, to that same tail

In addition, a global pool tunnel has been configured from each head end, to carry best-effort traffic to the same destinations. All four tunnels use the same tail router, even though they have different heads and differ in their passage through the midpoints. (Of course in the real world there would be many more midpoints than just the two shown here.)

All POS interfaces in this example are OC3, whose capacity is 155 Mbps.

Configuring a multi-destination guaranteed bandwidth service involves:

- Building a sub-pool MPLS-TE tunnel
- Configuring DiffServ QoS
- Configuring QoS Policy Propagation via BGP (QPPB)
- Mapping traffic onto the tunnels

All of these tasks are included in the following example.

## Configuration of Tunnel Head-1

First we recapitulate commands that establish a sub-pool tunnel (commands presented earlier on page 13) and now we also configure a global pool tunnel. Additionally, we present QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (With the 7500(VIP) router, Modular QoS CLI is used).

### Configuring the Pools and Tunnels

At the device level:

```

router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis router ospf 100
router-1(config-router)# net redistribute connected
49.0000.1000.0000.0010.00 network 10.1.1.0 0.0.0.255 area 0
router-1(config-router)# metric-style wide network 23.1.1.1 0.0.0.0 area
router-1(config-router)# is-type level-1 0
 mpls traffic-eng area 0

router-1(config-router)# mpls traffic-eng
level-1
[now one resumes the common command set]:

router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit

```

Create a virtual interface:

```

router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# exit

```

At the outgoing physical interface:

```

router-1(config)# interface pos4/0
router-1(config-if)# ip address 10.1.1.1 255.0.0.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:

```

```
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-1(config)# interface Tunnel1
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path1
router-1(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-1(config)# interface Tunnel2
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth 80000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
best-effort-path1
router-1(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-1(config)# ip explicit-path name gbs-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
router-1(config)# ip explicit-path name best-effort-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 25.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

## Configuring DiffServ QoS

At the inbound physical interface (in [Figure 3](#) this is FE4/1/0), packets received are rate-limited to:

- a. a rate of 30 Mbps
- b. a normal burst of 1 MB
- c. a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```
router-1(config)# interface FastEthernet4/1/0
router-1(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
conform-action set-mpls-exp-transmit 5 exceed-action drop
router-1(config-if)# bgp-policy destination ip-qos-map
router-1(config-if)# exit
```

At the device level create a class of traffic called “exp5-class” that has MPLS experimental bit set to 5:

```
router-1(config)# class-map match-all exp5-class
router-1(config-cmap)# match mpls experimental 5
router-1(config-cmap)# exit
```

Create a policy that creates a priority queue for “exp5-class”:

```
router-1(config)# policy-map core-out-policy
router-1(config-pmap)# class exp5-class
router-1(config-pmap-c)# priority 100000
router-1(config-pmap-c)# exit
router-1(config-pmap)# class class-default
router-1(config-pmap-c)# bandwidth 55000
router-1(config-pmap-c)# exit
router-1(config-pmap)# exit
```

The policy is applied to packets exiting the outbound interface POS4/0.

```
router-1(config)# interface POS4/0
router-1(config-if)# service-policy output core-out-policy
```

## Configuring QoS Policy Propagation via BGP

### For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-1(config)# ip bgp-community new-format
router-1(config)# router bgp 2
router-1(config-router)# no synchronization
router-1(config-router)# table-map set-qos-group
router-1(config-router)# bgp log-neighbor-changes
router-1(config-router)# neighbor 27.1.1.1 remote-as 2
router-1(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-1(config-router)# no auto-summary
router-1(config-router)# exit
```

### For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 so they will be mapped onto Tunnel #1 (the guaranteed bandwidth service tunnel). At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 100
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 100 permit ^5$
```

### For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 101
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
```

```
router-1(config)# ip as-path access-list 101 permit _5_
```

### For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match community 20
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip community-list 20 permit 100:1
```

### Mapping Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #1:

```
router-1(config)# ip route 29.1.1.1 255.255.255.255 Tunnel1
```

Map all best-effort traffic onto Tunnel #2:

```
router-1(config)# ip route 30.1.1.1 255.255.255.255 Tunnel2
```

## Configuration of Tunnel Head-2

As with the Head-1 device and interfaces, the following Head-2 configuration first presents commands that establish a sub-pool tunnel (commands presented earlier on page 13) and then also configures a global pool tunnel. After that it presents QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (Because this is a 7500 (VIP) router, Modular QoS CLI is used).

### Configuring the Pools and Tunnels

At the device level:

```
router-2(config)# ip cef distributed
router-2(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# router isis router ospf 100
router-2(config-router)# net redistribute connected
49.0000.1000.0000.0011.00
router-2(config-router)# metric-style wide network 11.1.1.0 0.0.0.255 area 0
router-2(config-router)# is-type level-1 network 22.1.1.1 0.0.0.0 area
 0
router-2(config-router)# mpls traffic-eng mpls traffic-eng area 0
level-1

[now one resumes the common command set]:

router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
```

```
router-2(config-if)# exit
```

At the outgoing physical interface:

```
router-2(config)# interface pos0/0
router-2(config-if)# ip address 11.1.1.1 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-2(config-if)# ip router isis
[and in all cases]:
router-2(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-2(config)# interface Tunnel3
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path2
router-2(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-2(config)# interface Tunnel4
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth 70000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
best-effort-path2
router-2(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-2(config)# ip explicit-path name gbs-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
router-2(config)# ip explicit-path name best-effort-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 25.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

## Configuring DiffServ QoS

At the inbound physical interface (in [Figure 3](#) this is FE2/1), packets received are rate-limited to:

- a. a rate of 30 Mbps
- b. a normal burst of 1 MB
- c. a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```
router-2(config)# interface FastEthernet2/1
router-2(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
conform-action set-mpls-exp-transmit 5 exceed-action drop
router-2(config-if)# bgp-policy destination ip-qos-map
router-1(config-if)# exit
```

At the device level create a class of traffic called “exp5-class” that has MPLS experimental bit set to 5:

```
router-2(config)# class-map match-all exp5-class
router-2(config-cmap)# match mpls experimental 5
router-2(config-cmap)# exit
```

Create a policy that creates a priority queue for “exp5-class”:

```
router-2(config)# policy-map core-out-policy
router-2(config-pmap)# class exp5-class
router-2(config-pmap-c)# priority 100000
router-2(config-pmap-c)# exit
router-2(config-pmap)# class class-default
router-2(config-pmap-c)# bandwidth 55000
router-2(config-pmap-c)# exit
router-2(config-pmap)# exit
```

The policy is applied to packets exiting interface POS0/0:

```
interface POS0/0
 service-policy output core-out-policy
```

As a result of all the above configuration lines, packets entering the Head-2 router via interface FE2/1 and destined for AS5, BGP community 100:1, or transiting AS5 will have their experimental field set to 5. It is assumed that no other packets entering this router (on any interface) are using this exp bit value. (If this cannot be assumed, an additional configuration must be added to mark all such packets with another experimental value.) When exiting this router via interface POS0/0, packets marked with experimental value 5 are placed into the priority queue.


**Note**

Packets entering the router via FE2/1 and exiting through POS0/0 enter as IP packets and exit as MPLS packets.

## Configuring QoS Policy Propagation via BGP

### For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-2(config)# ip bgp-community new-format
router-2(config)# router bgp 2
router-2(config-router)# no synchronization
router-2(config-router)# table-map set-qos-group
router-2(config-router)# bgp log-neighbor-changes
router-2(config-router)# neighbor 27.1.1.1 remote-as 2
router-2(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-2(config-router)# no auto-summary
router-2(config-router)# exit
```

### For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 so they will be mapped onto Tunnel #3 (the guaranteed bandwidth service tunnel). At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 100
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 100 permit ^5$
```

### For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 101
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 101 permit _5_
```

### For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match community 20
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip community-list 20 permit 100:1
```

### Mapping the Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #3:

```
router-2(config)# ip route 29.1.1.1 255.255.255.255 Tunnel13
```

Map all best-effort traffic onto Tunnel #4:

```
router-2(config)# ip route 30.1.1.1 255.255.255.255 Tunnel14
```

## Tunnel Midpoint Configuration [Mid-1]

All four interfaces on the midpoint router are configured very much like the outbound interface of the head router. The strategy is to have all mid-point routers in this Autonomous System ready to carry future as well as presently configured sub-pool and global pool tunnels.

### Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef distributed
```

router-3(config)# **mpls traffic-eng tunnels**  
 [now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> router-3(config)# <b>router isis</b> router-3(config-router)# <b>net</b> <b>49.0000.2400.0000.0011.00</b> router-3(config-router)# <b>metric-style wide</b> router-3(config-router)# <b>is-type level-1</b>  router-3(config-router)# <b>mpls traffic-eng</b> <b>level-1</b> router-3(config-router)# router-3(config-router)# router-3(config-router)# router-3(config-router)# </pre> | <pre> router ospf 100 redistribute connected network 10.1.1.0 0.0.0.255 area 0 network 11.1.1.0 0.0.0.255 area 0 network 24.1.1.1 0.0.0.0 area 0 network 12.1.1.0 0.0.0.255 area 0 network 13.1.1.0 0.0.0.255 area 0 mpls traffic-eng area 0 </pre> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set]:

```

router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit

```

Create a virtual interface:

```

router-3(config)# interface Loopback0
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# exit

```

At the physical interface level (ingress):

```

router-3(config)# interface pos2/1
router-3(config-if)# ip address 10.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

router-3(config)# interface pos1/1
router-3(config-if)# ip address 11.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the physical interface level (egress), through which two sub-pool tunnels currently exit:

```

router-3(config)# interface pos3/1
router-3(config-if)# ip address 12.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the physical interface level (egress), through which two global pool tunnels currently exit:

```

router-3(config)# interface pos4/1
router-3(config-if)# ip address 13.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000

```

```
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

## Tunnel Midpoint Configuration [Mid-2]

Both interfaces on this midpoint router are configured like the outbound interfaces of the Mid-1 router.

### Configuring the Pools and Tunnels

At the device level:

```
router-5(config)# ip cef distributed
router-5(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                                                                                                                                                                                                                                |                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-5(config)# router isis router-5(config-router)# net 49.2500.1000.0000.0012.00 router-5(config-router)# metric-style wide router-5(config-router)# is-type level-1 router-5(config-router)# mpls traffic-eng level-1 router-5(config-router)#</pre> | <pre>router ospf 100 redistribute connected network 13.1.1.0 0.0.0.255 area 0 network 14.1.1.0 0.0.0.255 area 0 network 25.1.1.1 0.0.0.0 area 0 mpls traffic-eng area 0</pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set]:

```
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit
```

Create a virtual interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit
```

At the physical interface level (ingress):

```
router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

At the physical interface level (egress):

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

## Tunnel Tail Configuration

The inbound interfaces on the tail router are configured much like the outbound interfaces of the midpoint routers:

### Configuring the Pools and Tunnels

At the device level:

```
router-4(config)# ip cef distributed
router-4(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right. In the case of OSPF, one must advertise two new loopback interfaces—29.1.1.1 and 30.1.1.1 in our example—which are defined in the QoS Policy Propagation section, further along on this page]:

|                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-4(config)# router isis router-4(config-router)# net 49.0000.2700.0000.0000.00 router-4(config-router)# metric-style wide router-4(config-router)# is-type level-1 router-4(config-router)# mpls traffic-eng level-1 router-4(config-router)# router-4(config-router)# router-4(config-router)# router-4(config-router)#</pre> | <pre>router ospf 100 redistribute connected network 12.1.1.0 0.0.0.255 area 0 network 14.1.1.0 0.0.0.255 area 0 network 27.1.1.1 0.0.0.0 area 0 network 29.1.1.1 0.0.0.0 area 0 network 30.1.1.1 0.0.0.0 area 0 mpls traffic-eng area 0</pre> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set, taking care to include the two additional loopback interfaces]:

```
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# mpls traffic-eng router-id Loopback1
router-4(config-router)# mpls traffic-eng router-id Loopback2
router-4(config-router)# exit
```

Create a virtual interface:

```
router-4(config)# interface Loopback0
router-4(config-if)# ip address 27.1.1.1 255.255.255.255
router-4(config-if)# exit
```

At the physical interface (ingress):

```
router-4(config)# interface pos2/1
router-4(config-if)# ip address 12.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

router-4(config)# interface pos2/2
router-4(config-if)# ip address 14.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
```

```
[and in all cases]:
router-4(config-if)# exit
```

## Configuring QoS Policy Propagation

On the tail device, one must configure a separate virtual loopback IP address for each class-of-service terminating here. The headend routers need these addresses to map traffic into the proper tunnels. In the current example, four tunnels terminate on the same tail device but they represent only two service classes, so only two additional loopback addresses are needed:

Create two virtual interfaces:

```
router-4(config)# interface Loopback1
router-4(config-if)# ip address 29.1.1.1 255.255.255.255
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit
router-4(config)# interface Loopback2
router-4(config-if)# ip address 30.1.1.1 255.255.255.255
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit
```

At the device level, configure BGP to send the community to each tunnel head:

```
router-4(config)# ip bgp-community new-format
router-4(config)# router bgp 2
router-4(config-router)# neighbor 23.1.1.1 send-community
router-4(config-router)# neighbor 22.1.1.1 send-community
router-4(config-router)# exit
```

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip rsvp bandwidth**
- **mpls traffic-eng ds-te bc-model**
- **mpls traffic-eng ds-te mode**
- **show mpls traffic-eng topology**
- **tunnel mpls traffic-eng bandwidth**

# Glossary

This section defines acronyms and words that may not be readily understood.

**AS**—Autonomous System. A collection of networks under a common administration, sharing a common routing strategy and identified by a unique 16-bit number (assigned by the Internet Assigned Numbers Authority).

**BGP**—Border Gateway Protocol. The predominant interdomain routing protocol. It is defined by RFC 1163. Version 4 uses route aggregation mechanisms to reduce the size of routing tables.

**CBR**—Constraint Based Routing. The computation of traffic paths that simultaneously satisfy label-switched path attributes and current network resource limitations.

**CEF**—Cisco Express Forwarding. A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

**CLI**—Command Line Interface. Cisco's interface for configuring and managing its routers.

**DS-TE**—Diff Serv-aware Traffic Engineering. The capability to configure two bandwidth pools on each link, a *global pool* and a *sub-pool*. MPLS traffic engineering tunnels using the sub-pool bandwidth can be configured with Quality of Service mechanisms to deliver guaranteed bandwidth services end-to-end across the network. Simultaneously, tunnels using the global pool can convey DiffServ traffic.

**flooding**—A traffic passing technique used by switches and bridges in which traffic received on an interface is sent out through all of the interfaces of that device except the interface on which the information was originally received.

**GB queue**—Guaranteed Bandwidth queue. A per-hop behavior (PHB) used exclusively by the strict guarantee traffic. If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used.

**Global Pool**—The total bandwidth allocated to an MPLS traffic engineering link.

**IGP**—Interior Gateway Protocol. An internet protocol used to exchange routing information within an autonomous system. Examples of common internet IGPs include IGRP, OSPF, and RIP.

**label-switched path (LSP) tunnel**—A configured connection between two routers, using label switching to carry the packets.

**IS-IS**—Intermediate System-to-Intermediate System. A link-state hierarchical routing protocol, based on DECnet Phase V routing, whereby nodes exchange routing information based on a single metric, to determine network topology.

**LCAC**—Link-level (per-hop) call admission control.

**LSP**—Label-switched path (see above).

*Also* Link-state packet—A broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSPs are used by the receiving routers to maintain their routing tables. Also called link-state advertisement (LSA).

**MPLS**—Multi-Protocol Label Switching (formerly known as Tag Switching). A method for directing packets primarily through Layer 2 switching rather than Layer 3 routing, by assigning the packets short fixed-length labels at the ingress to an MPLS cloud, using the concept of forwarding equivalence classes. Within the MPLS domain, the labels are used to make forwarding decisions mostly without recourse to the original packet headers.

**MPLS TE**—MPLS Traffic Engineering (formerly known as “RRR” or Resource Reservation Routing). The use of label switching to improve traffic performance along with an efficient use of network resources.

**OSPF**—Open Shortest Path First. A link-state, hierarchical IGP routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**RSVP**—Resource reSerVation Protocol. An IETF protocol used for signaling requests (to set aside internet services) by a customer before that customer is permitted to transmit data over that portion of the network.

**Sub-pool**—The more restrictive bandwidth in an MPLS traffic engineering link. The sub-pool is a portion of the link's overall global pool bandwidth.

**TE**—Traffic engineering. The application of scientific principles and technology to measure, model, and control internet traffic in order to simultaneously optimize traffic performance and network resource utilization.

**Note**

---

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS DiffServ Tunneling Modes

---

**First Published: November 25, 2002**

**Last Updated: March 20, 2006**

MPLS DiffServ Tunneling Modes allows service providers to manage the quality of service (QoS) that a router will provide to a Multiprotocol Label Switching (MPLS) packet in an MPLS network. MPLS DiffServ Tunneling Modes conforms to the IETF draft standard for Uniform, Short Pipe, and Pipe modes. It also conforms to Cisco-defined extensions for scalable command line interface (CLI) management of those modes at customer edge, provider edge, and core routers.

The following features are supported on MPLS DiffServ Tunneling Modes:

- MPLS per-hop behavior (PHB) layer management.
- There is improved scalability of the MPLS layer management by control on managed customer edge (CE) routers.
- MPLS can “tunnel” a packet’s QoS (that is, the QoS is transparent from edge to edge).
- The MPLS experimental (MPLS EXP) field can be marked differently and independently of the PHB marked in the IP Precedence or differentiated services code point (DSCP) field.
- There are three MPLS QoS tunneling modes for the operation and interaction between the DiffServ marking in the IP header and the DiffServ marking in the MPLS header: Pipe mode with an explicit NULL LSP, Short Pipe mode, and Uniform mode. Pipe mode with an explicit NULL LSP and Short Pipe mode allow an MPLS network to transparently tunnel the DiffServ marking of packets.

MPLS DiffServ Tunneling Modes has the following benefits:

- Tunneling modes provide added QoS functionality by the creative manipulation of the MPLS EXP field during label imposition, forwarding, and label disposition.
- Tunneling modes provide a common set of PHBs to different service provider customers.
- Pipe mode provides transparency and customized edge service.
- Pipe mode with an explicit NULL LSP improves the scalability of management by performing per-customer packet metering and marking closer to the service provider’s customer networks.
- Pipe mode with an explicit NULL LSP provides QoS transparency by ensuring that customer’s packets will not be re-marked in the service provider’s network.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- In Pipe mode with an explicit NULL LSP, the explicit NULL LSP applies the service provider's PHBs on the ingress CE-to-PE link.
- In Pipe mode with an explicit NULL LSP, the service provider's PHBs are applied on the egress PE-to-CE link.
- Short Pipe mode provides transparency, standard edge service, and scalability.
- Short Pipe mode provides PHB management on the PE router. The customer's set of PHBs is applied on both the egress PE-to-CE link and on the ingress CE-to-PE link.
- Customers are likely to use Uniform mode if they have no markings or few markings. The customer lets the Internet service provider (ISP) mark the packets and retain their markings.
- In Uniform mode, all changes to QoS markings are reflected at each level (that is, IGP, BGP, and IP).
- In Uniform mode, if a QoS marking is changed in the MPLS network, it is changed in the IP packet too.

#### History for the MPLS DiffServ Tunneling Modes Feature

| Release                  | Modification                                                   |
|--------------------------|----------------------------------------------------------------|
| 12.2(13)T                | This feature was introduced.                                   |
| 12.2(28)SB               | This feature was integrated into Cisco IOS Release 12.2(28)SB. |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.  |

## Contents

- [Prerequisites for MPLS DiffServ Tunneling Modes, page 2](#)
- [Restrictions for MPLS DiffServ Tunneling Modes, page 3](#)
- [Information About MPLS DiffServ Tunneling Modes, page 3](#)
- [How to Configure MPLS DiffServ Tunneling Modes, page 17](#)
- [Configuration Examples for MPLS DiffServ Tunneling Modes, page 40](#)
- [Additional References, page 46](#)
- [Command Reference, page 48](#)
- [Glossary, page 48](#)

## Prerequisites for MPLS DiffServ Tunneling Modes

- Set up the network to run MPLS.
- Enable IP Cisco Express Forwarding (CEF).
- Define the Service Level Agreement (SLA).
- Know each customer's per-hop behavior.
  - What do customers expect you to provide?
  - Are customers going to mark the traffic?

- Identify whether the customer's traffic will be voice or data.
- Determine the topology and interfaces that need to be configured.
- Understand how IP and MPLS packets are forwarded.

## Restrictions for MPLS DiffServ Tunneling Modes

- A single label-switched path (LSP) can support up to eight classes of traffic (that is, eight PHBs) because the MPLS EXP field is a 3-bit field.
- MPLS DiffServ Tunneling Modes does not support L-LSPs. Only E-LSPs are supported.

## Information About MPLS DiffServ Tunneling Modes

To configure MPLS DiffServ Tunneling Modes, you need to understand the following concepts:

- [QoS and Its Use in MPLS Tunneling, page 3](#)
- [Tunneling Modes for MPLS DiffServ, page 6](#)
- [MPLS PHB Layer Management, page 7](#)
- [Tunneling Modes Operation, page 8](#)

## QoS and Its Use in MPLS Tunneling

This section includes the following subsections:

- [What is QoS?, page 3](#)
- [Services Supported by MPLS QoS, page 4](#)
- [Providing QoS to an IP Packet, page 5](#)
- [Providing QoS to an MPLS Packet, page 5](#)
- [DiffServ as a Standardization of QoS, page 6](#)

## What is QoS?

Critical applications must be guaranteed the network resources they need, despite a varying network traffic load. QoS is a set of techniques that manage the following:

- Network bandwidth—Noncritical traffic is prevented from using bandwidth that critical applications need. The main cause of congestion is lack of bandwidth.
- Network delay (also called latency)—The time required to move a packet from the source to the destination over a path.
- Jitter—The interpacket delay variance; that is, the difference between interpacket arrival and departure. Jitter can cause data loss.
- Packet loss—The dropping of packets.

Service providers offering MPLS VPN and traffic engineering (TE) services can provide varying levels of QoS for different types of network traffic. For example, Voice-over-IP (VoIP) traffic receives service with an assured minimum of delay, whereas e-commerce traffic might receive a minimum bandwidth guarantee (but not a delay guarantee).

For more information about QoS, see the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2 and the *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.2.

## Services Supported by MPLS QoS

MPLS QoS supports the following services:

- Class-based weighted fair queuing (CBWFQ)—Provides queuing based on defined classes, with no strict priority queue available for real-time traffic. Weighted fair queuing allows you to define traffic classes based on match criteria. Once a class has been defined, you can assign characteristics to the class. For example, you can designate the minimum bandwidth delivered to the class during congestion.
- Low latency queuing (LLQ)—Provides strict priority queuing, which allows delay-sensitive data such as voice to be processed and sent first, before packets in other queues are processed. This provides preferential treatment to delay-sensitive data over other traffic.
- Weighted fair queuing (WFQ)—An automated scheduling system that uses a queuing algorithm to ensure fair bandwidth allocation to all network traffic. Weighted fair queuing is based on a relative bandwidth applied to each of the queues.

- **Weighted random early detection (WRED)**—RED is a congestion avoidance mechanism that controls the average queue size by indicating to the end hosts when they should temporarily stop sending packets. A small percentage of packets is dropped when congestion is detected and before the queue in question overflows completely.

The weighted aspect of WRED ensures that high-precedence traffic has lower loss rates than other traffic during congestion. WRED can be configured to discard packets that have certain markings. When a packet comes into a router, it is assigned an internal variable that is called a discard class. If desired, you can set the discard class at the input interface. At the output interface, the router can be configured to use the discard class for WRED instead of the MPLS EXP field.

### Service Level Agreements Used in MPLS Tunneling

The service provider has an SLA with each customer. Each customer can have a different SLA. For example, the SLA for customer C1 may allow 256 kilobits of bandwidth for TCP packets (such as FTP packets or Telnet packets) and 1 megabyte of voice traffic per second. If the customer transmits 1 megabyte of voice traffic per second, the service provider delivers it to the other side of the customer's network. If the customer transmits more, the excess traffic is considered out-of-rate traffic and may or may not be discarded.

If the service provider experiences congestion, the service provider decides how to handle those packets. For example, the service provider may drop packets or give them less bandwidth. The PHB may be to drop a packet or to give it 20 percent of the link bandwidth.

The PHB that the service provider provides for a packet may be different from the PHB that the customer wants traffic to have in their network. The customer may be providing QoS at the output interface of each router in their network. However, the customer may be providing a different amount of bandwidth on those links than the service provider will provide. For example, a customer may give 50 percent of the link bandwidth to voice. The service provider may want to give only 10 percent of the link bandwidth to voice.

## Providing QoS to an IP Packet

In an IP packet, the QoS that a router must provide has traditionally been designated in the IP Precedence field, which is the first three bits of the type of service (ToS) byte in the header of an IP packet. The IP Precedence and the differentiated services code point (DSCP) in an IP packet define the class. They may also designate the discard profile within a class. The DSCP is specified in the IETF standard for DiffServ. It is a new IETF standard for QoS.

Although some people still use the IP Precedence field, others use the DSCP to indicate the PHB that will be provided to an IP packet.

After label imposition, a configurable mapping function marks an equivalent PHB into the 3-bit MPLS EXP field value based on the IP Precedence or the IP DSCP marking.

## Providing QoS to an MPLS Packet

In an MPLS packet, the PHB is marked in the MPLS EXP field within the MPLS label entry.

The EXP bits are similar in function to the IP Precedence and the DSCP in the IP network. The EXP bits generally carry all the information encoded in the IP Precedence or the DSCP.

The edge LSR that imposes the MPLS header sets the MPLS EXP field to a value.

## DiffServ as a Standardization of QoS

DiffServ is a QoS architecture for IP networks. Packets within a DiffServ-enabled network may be classified into classes such as premium, gold, silver, or bronze based on QoS requirements. For example, VoIP packets may be grouped into the premium class, and e-commerce HTTP packets may be grouped into the gold class.

Each class has a marking associated with it. This makes packet classification extremely scalable and assures appropriate bandwidth and delay guarantees in the network. When packets enter the network, they are marked based on classification policies at the network boundary routers. The boundary routers also apply traffic conditioning functions to control the amount of traffic entering the network. Traffic conditioning includes the following:

- Shaping—Smoothing the rate at which packets are sent into the network
- Policing—Dropping packets that exceed a subscribed-to-rate, or re-marking packets exceeding the rate so that the probability of dropping them increases when there is congestion

Each router within the network then applies different queuing and dropping policies on each packet based on the marking that the packet carries.

For more information about DiffServ, see the *Cisco IOS Switching Services Configuration Guide*, Release 2.2.

## Tunneling Modes for MPLS DiffServ

Tunneling is the ability of QoS to be transparent from one edge of a network to the other edge of the network. A tunnel starts where there is label imposition. A tunnel ends where there is label disposition; that is, where the label is popped off of the stack and the packet goes out as an MPLS packet with a different PHB layer underneath or as an IP packet with the IP PHB layer.

There are three ways to forward packets through a network:

- Pipe mode with an explicit NULL LSP
- Short Pipe mode
- Uniform mode

Pipe mode and Short Pipe mode provide QoS transparency. With QoS transparency, the customer's IP marking in the IP packet is preserved.

**Note**

---

The only difference between Pipe mode and Short Pipe mode is which PHB is used on the service provider's egress edge router. In Pipe mode with an explicit NULL LSP, QoS is done on the PE-to-CE link based on the service provider's PHB markings. The egress LSR still uses the marking that was used by intermediate LSRs.

---

All three tunneling modes affect the behavior of edge and penultimate label switching routers (LSRs) where labels are pushed (put onto packets) and popped (removed from packets). They do not affect label swapping at intermediate routers. A service provider can choose different types of tunneling modes for each customer.

Following is a brief description of each tunneling mode:

- Pipe mode with an explicit NULL LSP—QoS is done on the output interface of the PE router based on the received MPLS EXP field, even though one or more label entries have been popped. The IP Precedence field, EXP bits, and the DSCP field are not altered when they travel from the ingress to the egress of the MPLS network.

Any changes to the packet marking within the MPLS network are not permanent and do not get propagated when the packet leaves the MPLS network. The egress LSR still uses the marking that was used by intermediate provider core (P) routers. However, the egress provider edge (PE) router has to remove labels imposed on the original packet. To preserve the marking carried in the labels, the edge PE router keeps an internal copy of the marking before removing the labels. This internal copy is used to classify the packet on the outbound interface (facing the CE) after the labels are removed.

For a detailed description, see the [“Pipe Mode with an Explicit NULL LSP” section on page 8](#).

For the configuration procedure, see the [“Configuring Pipe Mode with an Explicit NULL LSP” section on page 18](#).

For an example, see the [“Pipe Mode with an Explicit NULL LSP Configuration Example” section on page 41](#).

- Short Pipe mode—In Short Pipe mode, the egress PE router uses the original packet marking instead of the marking used by the intermediate P routers.

For a detailed description, see the [“Short Pipe Mode” section on page 12](#).

For the configuration procedure, see the [“Configuring Short Pipe Mode” section on page 26](#).

For an example, see the [“Short Pipe Mode Configuration Example” section on page 43](#).

- Uniform mode—In Uniform mode, the marking in the IP packet may be manipulated to reflect the service provider’s QoS marking in the core.

For a detailed description, see the [“Uniform Mode” section on page 15](#).

For the configuration procedure, see the [“Configuring Uniform Mode” section on page 32](#).

For an example, see the [“Uniform Mode Configuration Example” section on page 44](#).

## MPLS PHB Layer Management

Through the network of routers, the MPLS EXP field can be marked differently and independently of the PHB marked in the IP Precedence or the DSCP field. A service provider can choose from existing classification criteria, including or excluding the IP PHB marking, to classify packets into a different PHB which is then marked only in the MPLS EXP field during label imposition.

Layer management is the ability to apply an additional layer of PHB marking to a packet. The PHB is the behavior of a packet at a router (that is, the unique discard and scheduling behavior that is applied to a packet). Layer management can occur at a service provider-managed CE router or at the service provider edge (PE) router.

If a packet arrives in a network as an IP packet, it may already have a PHB layer that is represented by a marking in the ToS byte. The marking can be IP Precedence bits or the DSCP.

If a packet arrives as an MPLS packet, it already has the following two PHB layers:

- IP layer
- MPLS layer, where the marking is in the MPLS EXP field of the topmost label entry

At a given hop, one PHB layer can be added to a packet. If only one label is being pushed onto the packet, the marking for the PHB layer being added is contained in only one label.

If two or more labels are being pushed onto a packet, the PHB layer being added is marked with the same MPLS EXP field in all of the label entries being pushed on at that time.

## Tunneling Modes Operation



### Note

---

Cisco IOS allows a flexible configuration. You can configure the PHB definition of the MPLS EXP field differently from the PHB definition of the IP Precedence and DSCP.

---

A service provider may or may not care about the PHB marking of their customer's packet. For example, in customer C1's network, an IP Precedence value of 5 may mean voice. In customer C2's network, an IP Precedence value of 3 may mean voice. The service provider does not want to have two different IP Precedence values for voice. If the service provider has a large number of customers, there could be "many" values for voice. There are only eight possible EXP values.

To deal with different IP Precedence values representing the same PHB (in our example, for voice), the service provider does the following:

1. Arbitrarily chooses a common MPLS EXP field value to represent a PHB. For example, 2 can represent voice.
2. Looks at the packets of each customer. The service provider may look at the IP Precedence field value or at the UDP port number for voice, which is constant in every network.
3. For all customers, sets each voice packet to the MPLS EXP field value 2 on all the service provider's customer ports. Consequently, each router in the service provider's network only has to look for the MPLS EXP field value 2 for voice.

Another solution would be to set the DSCP value to 2, but that would alter the customer's PHB. MPLS DiffServ tunneling modes achieve the same results without altering the DSCP value.

This section illustrates and describes the following:

- [Pipe Mode with an Explicit NULL LSP, page 8](#)
- [Short Pipe Mode, page 12](#)
- [Uniform Mode, page 15](#)

## Pipe Mode with an Explicit NULL LSP

This section describes the following:

- [Pipe Mode with an Explicit NULL LSP Overview, page 9](#)
- [Pipe Mode with an Explicit NULL LSP Operating Procedure, page 11](#)

**Pipe Mode with an Explicit NULL LSP Overview**

Pipe mode with an explicit NULL LSP has the following characteristics:

- The QoS tunnel goes from the ingress CE router through the PE router to the egress CE router.
- There is an explicit NULL LSP from the CE router to the PE router. The label entry contains an MPLS EXP field, but does not carry a label value for forwarding purposes. It contains a zero (a null label value) for all packets going to the ingress PE router.
- The egress PE router removes the label entry and forwards packets as IP, but QoS is done on the output interface based on the MPLS EXP field received by the egress PE router.
- The service provider does not overwrite the IP Precedence value in the service provider's network.

[Figure 1](#) shows an overview of Pipe mode with an explicit NULL LSP.

**Figure 1** *Pipe Mode with an Explicit NULL LSP Overview*



---

**Note** PE1 and PE2 are at the boundaries between the MPLS network and the IP network.

---

Figure 1 illustrates the following:

1. An IP packet arrives at C1, CE1 with a DSCP value of 1.
2. C2, CE1 sets the MPLS EXP field value to 5 during label imposition of the null label.
3. The packet goes through the service provider's network with the MPLS EXP field value set to 5.
4. Each router in the service provider's network looks at the MPLS EXP field and does QoS based on that value.
5. When the packet gets to the egress PE router going back into C1's network, it does QoS based on the packet's MPLS EXP field even though the packet is transmitted as an IP packet.

#### Pipe Mode with an Explicit NULL LSP Operating Procedure

Figure 2 illustrates the operation of Pipe mode with an explicit NULL LSP for Customer 1, when MPLS VPN is enabled. Since VPN is enabled, there are two MPLS label entries. Otherwise, there would be only one entry. The functionality would be similar for Customer 2, but the DSCP value would be 3.

**Figure 2** *Pipe Mode with an Explicit NULL LSP Operation with MPLS VPN Enabled*



Pipe mode with an explicit NULL LSP functions as follows. The circled numbers at the bottom of the illustration correspond to the step numbers.

1. IP packets arrive at the router CE1, the managed CE router, with a DSCP value of 1.
2. An explicit NULL label entry is imposed onto the packet that contains an EXP value of 5.
3. The packet is transmitted to PE1 on the explicit NULL LSP.
4. The PE1 router saves the value of the MPLS EXP field and removes the explicit NULL entry. The PE1 router then imposes new labels onto the IP packet. Each label entry is set to the saved MPLS EXP field 5.
5. The packet is transmitted to P1.
6. At P1, the received EXP value is copied into the swapped label entry.
7. The packet is transmitted to P2.

8. At P2, the topmost label is popped, exposing a label entry that also has an EXP value of 5.
9. The packet is transmitted to PE2.
10. PE2 stores the value of the MPLS EXP field in the qos-group and discard-class variables, and removes the label entry from the packet.
11. While transmitting the packet to CE2, PE2 does QoS on its egress interface based on the saved value of the MPLS EXP field (qos-group and discard-class).
12. The IP packet arrives at the CE2 router.

## Short Pipe Mode

This section describes the following:

- [Short Pipe Mode Overview, page 12](#)
- [Short Pipe Mode Operating Procedure, page 14](#)

### Short Pipe Mode Overview

Short Pipe mode has the following characteristics:

- The QoS tunnel goes from the ingress PE router to the egress PE router.
- The egress PE router transmits packets as IP and QoS is done on the output interface based on the IP DSCP or IP Precedence value.
- The service provider does not overwrite the DSCP or IP Precedence value in the service provider's network.

[Figure 3](#) shows an overview of Short Pipe mode.

**Figure 3**      **Short Pipe Mode Overview**



**Note**

---

PE1 and PE2 are at the boundaries between the MPLS network and the IP network.

---

Figure 3 shows the following:

1. An IP packet arrives at C1, CE1 with a DSCP value of 1.
2. C1, CE1 transmits the IP packet to C1, PE1.
3. C1, PE1 sets the MPLS EXP field value to 5 during label imposition of the VPN label entries.
4. The packet goes through the service provider's network with the MPLS EXP field value set to 5.
5. Each router in the service provider's network looks at the MPLS EXP field and does QoS based on that value.
6. When the packet gets to the egress PE router going back into C1's network, it does QoS based on the IP DSCP field.

### Short Pipe Mode Operating Procedure

Figure 4 illustrates Short Pipe mode.

**Figure 4**      **Short Pipe Mode Operation**



Short Pipe mode functions as follows. The circled numbers at the bottom of the illustration correspond to the step numbers.

1. C1, CE1 transmits an IP packet to PE1 with an IP DSCP value of 1.
2. PE1 sets the MPLS EXP field to 5 in the imposed label entries.
3. PE1 transmits the packet to P1.
4. P1 sets the MPLS EXP field value to 5 in the swapped label entry.
5. P1 transmits the packet to P2.
6. P2 pops the IGP label entry.
7. P2 transmits the packet to PE2.
8. PE2 pops the BGP label.
9. PE2 transmits the packet to C1, CE2, but does QoS based on the IP DSCP value.

## Uniform Mode

This section describes the following:

- [Uniform Mode Overview, page 15](#)
- [Uniform Mode Operating Procedure, page 15](#)

### Uniform Mode Overview

In a label, the MPLS EXP field is not the same as the label value.

The topmost label entry contains the following:

- Label value, which contains labels and other information, to forward the packet.
- MPLS EXP field, which only pertains to the QoS of the packet, not the route. The EXP field value is not advertised. Its value comes from the way that the packet is received.

In Uniform mode, packets are treated uniformly in the IP and MPLS networks; that is, the IP Precedence value and the MPLS EXP bits always are identical. Whenever a router changes or recolors the PHB of a packet, that change must be propagated to all encapsulation markings. The propagation is performed by a router only when a PHB is added or exposed due to label imposition or disposition on any router in the packet's path. The color must be reflected everywhere, at all levels. For example, if a packet's QoS marking is changed in the MPLS network, the IP QoS marking reflects that change.

Uniform mode functions as follows:

- In both the MPLS-to-MPLS path and the MPLS-to-IP path, the PHBs of the topmost popped label are copied into the new top label or into the IP DSCP if no label remains.
- There can be a maximum of eight PHBs.
- If the PHBs are enclosed using more than the three Precedence bits, you must map DSCP to MPLS at the entry to the MPLS cloud.
- When packets leave the MPLS cloud, you must remap from the MPLS EXP value to the DSCP field in the IP header.

### Uniform Mode Operating Procedure

[Figure 5](#) illustrates the operation of Uniform mode.

**Figure 5** *Uniform Mode Operation*



The procedure varies according to whether there are IP Precedence bit markings or DSCP markings.

The following actions occur if there are IP Precedence bit markings:

1. IP packets arrive in the MPLS network at PE1, the service provider edge router.
2. A label is copied onto the packet.
3. If the MPLS EXP field value is recolorored (for example, if the packet becomes out-of-rate because too many packets are being transmitted), that value is copied to the IGP label. The value of the BGP label is not changed.
4. At the penultimate hop, the IGP label is removed. That value is copied into the next lower level label.
5. When all MPLS labels have been removed from the packet which is sent out as an IP packet, the IP Precedence or DSCP value is set to the last changed EXP value in the core.

Following is an example when there are IP precedence bit markings:

1. At CE1 (customer equipment 1), the IP packet has an IP Precedence value of 5.
2. When the packet arrives in the MPLS network at PE1 (the service provider edge router), the IP Precedence value of 5 is copied to the imposed label entries of the packet.
3. The MPLS EXP field in the IGP label header might be changed within the MPLS core (for example, at P1).



**Note**

---

Since the IP Precedence bits are 5, the BGP label and the IGP label also contain 5 because in Uniform mode the labels always are identical. The packet is treated uniformly in the IP and MPLS networks.

---

4. At P2, when the IGP label is removed, the MPLS EXP field in this label entry is copied into the underlying BGP label.
5. At PE2, when the BGP label is popped, the EXP field in this label header is copied into the IP Precedence field of the underlying IP header.

## How to Configure MPLS DiffServ Tunneling Modes

This section contains the following procedures:

- [Determining Which Tunneling Mode is Appropriate, page 17](#) (required)
- [Setting the MPLS EXP field, page 17](#) (optional)
- [Configuring Pipe Mode with an Explicit NULL LSP, page 18](#) (optional)
- [Configuring Short Pipe Mode, page 26](#) (optional)
- [Configuring Uniform Mode, page 32](#) (optional)



**Note**

---

You can configure only one of the tunneling modes.

---

### Determining Which Tunneling Mode is Appropriate

- If there are managed customer edge (CE) routers, we recommend that you use Pipe mode with an explicit NULL LSP so that there is service provider PHB on the PE-to-CE link.
- If there is no managed CE router, we recommend that you use Short Pipe mode.
- If there are no markings or few markings, customers are likely to use Uniform mode.

### Setting the MPLS EXP field

There are two ways to set the MPLS EXP field:

- Use the **set mpls experimental topmost** command to set the topmost label entry's value directly in the packet on the input and/or output interfaces.
- Use the **set mpls experimental imposition** command on the input interface to set the pushed label entry's value during label imposition.

By default, the label edge router copies the IP Precedence of the IP packet to the MPLS EXP field in all pushed label entries.

You can optionally map the IP Precedence or DSCP field to the MPLS EXP field in the MPLS header by using the **set mpls experimental imposition** command.

## Configuring Pipe Mode with an Explicit NULL LSP

This section describes how to configure the following:

- [Ingress CE Router—Customer Facing Interface, page 18](#)
- [Ingress CE Router—PE Facing Interface, page 19](#)
- [Ingress PE Router—P Facing Interface, page 21](#)
- [P Router—P Facing Interface, page 22](#)
- [Egress PE Router—P Facing Interface, page 24](#)
- [Egress PE Router—Customer Facing Interface, page 25](#)

For examples, see the “[Pipe Mode with an Explicit NULL LSP Configuration Example](#)” section on [page 41](#).

**Note**

---

The steps that follow show one way, but not the only way, to configure Pipe Mode with an Explicit NULL LSP.

---

### Ingress CE Router—Customer Facing Interface

This procedure configures a policy map to set the MPLS EXP field in imposed label entries.

#### SUMMARY STEPS

1. **class-map** *class-name*
2. **match ip dscp** *dscp-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
6. **interface** *type slot/port*
7. **service-policy input** *name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map IP-AF11                                                                                                                                                                                                                                                                                            | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 2 | <b>match ip dscp</b> <i>dscp-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match ip dscp 4                                                                                                                                                                                                                                                                                   | Uses the DSCP values as the match criteria for control plane traffic and other traffic that will be transmitted as IP.                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map set-MPLS-PHB                                                                                                                                                                                                                                                                                           | Configures the QoS policy for packets that match the class or classes.                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class IP-AF11                                                                                                                                                                                                                                                                                              | Associates the traffic class with the service policy.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 5 | <b>police</b> <i>bps</i> [ <i>burst-normal</i> ] [ <i>burst-max</i> ]<br><b>conform-action</b> <i>action</i> <b>exceed-action</b> <i>action</i><br>[ <b>violate-action</b> <i>action</i> ]<br><br><b>Example:</b><br>Router(config-p-map-c)# police 8000<br>conform-action<br>set-mpls-experimental-imposition-transmit 4<br>exceed-action<br>set-mpls-experimental-imposition-transmit 2 | Configures the Traffic Policing feature, including the following: <ul style="list-style-type: none"> <li>Action to take on packets that conform to the rate limit specified in the SLA (service level agreement)</li> <li>Action to take on packets that exceed the rate limit specified in the SLA</li> </ul> At the <i>action</i> field, enter <b>set-mpls-experimental-imposition</b> <i>value</i> , where <i>value</i> is the value to which the MPLS EXP field will be set. |
| Step 6 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                                                                                                                                                                                                                                                                                   | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number.                                                                                                                                                                                                                                                                |
| Step 7 | <b>service-policy input</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy input<br>set-MPLS-PHB                                                                                                                                                                                                                                                                 | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                                                                                                                                                                                                                                                                                        |

## Ingress CE Router—PE Facing Interface

This procedure classifies packets based on their MPLS EXP field and provides appropriate discard and scheduling treatments.

## SUMMARY STEPS

1. **class-map** *match-any class-name*

2. **match mpls experimental topmost** *mpls-values*
3. **match ip dscp** *dscp-values*
4. **policy-map** *name*
5. **class** *class-name*
6. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
7. **random-detect**
8. **interface** *type slot/port*
9. **service-policy output** *name*
10. **mpls ip encapsulate explicit-null**

## DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map match-any</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map match-any MPLS-AF1                           | Specifies that packets must meet one of the match criteria to be considered a member of the traffic class.                                                                   |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 2 4 | Matches up to eight MPLS EXP field values. Puts matching packets into the same class.                                                                                        |
| Step 3 | <b>match ip dscp</b> <i>dscp-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match ip dscp 4                                       | Uses the DSCP values as the match criteria for control plane traffic and other traffic that will be transmitted as IP.                                                       |
| Step 4 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos                                                 | Configures the QoS policy for packets that match the class or classes.                                                                                                       |
| Step 5 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class MPLS-AF1                                                 | Associates the traffic class with the service policy.                                                                                                                        |
| Step 6 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }                                                                    | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth. |
| Step 7 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                          | Applies WRED to the policy based on the IP Precedence or the MPLS EXP field value.                                                                                           |

|         | Command or Action                                                                                                       | Purpose                                                                                                                                                                                                           |
|---------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                 | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 9  | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output output-qos  | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                             |
| Step 10 | <b>mpls ip encapsulate explicit-null</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip encapsulate explicit-null | Encapsulates with an explicit NULL label header all packets forwarded from the interface or subinterface.                                                                                                         |

## Ingress PE Router—P Facing Interface

In this procedure, the default label swap behavior copies the received MPLS EXP field value to the output MPLS EXP field.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
6. **random-detect**
7. **interface** *type slot/port*
8. **service-policy output** *name*

### DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map MPLS-AF1                                               | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                    |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 2 4 | Specifies the MPLS values to use as match criteria against which packets are checked to determine if they belong to the class. |

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos                                                     | Configures the QoS policy for packets that match the class or classes.                                                                                                                                            |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class MPLS-AF1                                                     | Associates the traffic class with the service policy.                                                                                                                                                             |
| Step 5 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }<br><br><b>Example:</b><br>Router(config-p-map-c)# bandwidth percent 40 | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.                                      |
| Step 6 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                              | Applies WRED to the policy based on the IP Precedence or the MPLS EXP field value.                                                                                                                                |
| Step 7 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                                           | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 8 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output output-qos                            | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                             |

## P Router—P Facing Interface

This procedure classifies packets based on their MPLS EXP field and provides appropriate discard and scheduling treatments.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **set mpls experimental topmost** *value*
6. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
7. **random-detect**
8. **interface** *type slot/port*
9. **service-policy output** *name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map MPLS-AF1                                                   | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                                                       |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 2 4     | Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class.                                                                          |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos                                                     | Configures the QoS policy for packets that match the class or classes.                                                                                                                                            |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class MPLS-AF1                                                     | Associates the traffic class with the service policy.                                                                                                                                                             |
| Step 5 | <b>set mpls experimental topmost</b> <i>value</i><br><br><b>Example:</b><br>Router(config-p-map-c)# set mpls experimental topmost 3               | Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces. This command is optional.                                                                                   |
| Step 6 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }<br><br><b>Example:</b><br>Router(config-p-map-c)# bandwidth percent 40 | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.                                      |
| Step 7 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                              | Applies WRED to the policy based on the IP Precedence or the MPLS EXP field value.                                                                                                                                |
| Step 8 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                                           | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 9 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output output-qos                            | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                             |

## Egress PE Router—P Facing Interface

In this procedure, the qos-group and discard-class convey a packet's PHB to the output interface. The qos-group and discard-class will be used for QoS classification and then will be discarded. The output IP packet's ToS field will not be overwritten.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **set qos-group** *qos-group-value*
6. **set discard-class** *value*
7. **interface** *type slot/port*
8. **service-policy input** *name*

### DETAILED STEPS

|        | Command or Action                                                                                                                           | Purpose                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map MPLS-AF11                                            | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                           |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 4 | Specifies the packet characteristics that will be matched to the class.                                                                               |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map set-PHB                                                  | Configures the QoS policy for packets that match the class or classes.                                                                                |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class MPLS-AF11                                              | Associates the traffic class with the service policy.                                                                                                 |
| Step 5 | <b>set qos-group</b> <i>qos-group-value</i><br><br><b>Example:</b><br>Router(config-p-map-c)# set qos-group 1                               | Sets a group ID that can be used later to classify packets. Valid values are from 0 to 99.                                                            |
| Step 6 | <b>set discard-class</b> <i>value</i><br><br><b>Example:</b><br>Router(config-p-map-c)# set discard-class 1                                 | Marks a packet with a discard-class value. Specifies the type of traffic that will be dropped when there is congestion. Valid values are from 0 to 7. |

|        | Command or Action                                                                                                 | Purpose                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0           | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 8 | <b>service-policy input</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy input set-PHB | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                         |

## Egress PE Router—Customer Facing Interface

This procedure classifies a packet according to the QoS group ID and determines a packet's discard treatment according to the discard-class attribute.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match qos-group** *qos-group-value*
3. **policy-map** *name*
4. **class** *class-name*
5. **bandwidth** { *bandwidth-kbps* | **percent** *percent* }
6. **random-detect discard-class-based**
7. **interface** *type slot/port*
8. **mpls ip**
9. **service-policy output** *name*

### DETAILED STEPS

|        | Command or Action                                                                                               | Purpose                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map Local-AF1                | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class. |
| Step 2 | <b>match qos-group</b> <i>qos-group-value</i><br><br><b>Example:</b><br>Router(config-c-map)# match qos-group 1 | Identifies a specified QoS group value as a match criteria.                                 |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos                   | Configures the QoS policy for packets that match the class or classes.                      |

|        | Command or Action                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <code>class class-name</code><br><br><b>Example:</b><br>Router(config-p-map)# class Local-AF1                                         | Associates the traffic class with the service policy.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 5 | <code>bandwidth {bandwidth-kbps   percent percent}</code><br><br><b>Example:</b><br>Router(config-p-map-c)# bandwidth percent 40      | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.                                                                                                                                                                                                                                                                                                             |
| Step 6 | <code>random-detect discard-class-based</code><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect<br>discard-class-based | Bases WRED on the discard class value of a packet.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7 | <code>interface type slot/port</code><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                                | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number.                                                                                                                                                                                                                                                                        |
| Step 8 | <code>mpls ip</code><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                                             | Enables MPLS forwarding of IP version 4 (IPv4) packets along normally routed paths for a particular interface.<br><br><b>Note</b> You must issue the <code>mpls ip</code> command on this interface to receive packets with an explicit-NULL label from the CE router. The <code>mpls ip</code> command is not configured on the CE router's interface connected to this interface and therefore no LDP nor other label distribution protocol sessions will be established on this link. |
| Step 9 | <code>service-policy output name</code><br><br><b>Example:</b><br>Router(config-if)# service-policy output<br>output-qos              | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                                                                                                                                                                                                                                                                                                    |

## Configuring Short Pipe Mode

This section describes how to configure the following:

- [Ingress PE Router—Customer Facing Interface, page 27](#)
- [Ingress PE Router—P Facing Interface, page 28](#)
- [P Router—P Facing Interface, page 29](#)
- [Egress PE Router—Customer Facing Interface, page 31](#)

For examples, see the “Short Pipe Mode Configuration Example” section on page 43.



### Note

The steps that follow show one way, but not the only way, to configure Short Pipe mode.

## Ingress PE Router—Customer Facing Interface

This procedure configures a policy map to set the MPLS EXP field in imposed label entries.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match ip dscp** *dscp-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
6. **interface** *type slot/port*
7. **service-policy input** *name*

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map IP-AF11                                                                                                                                                                                                                                                                                            | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>match ip dscp</b> <i>dscp-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match ip dscp 4                                                                                                                                                                                                                                                                                   | Uses the DSCP values as the match criteria.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map set-MPLS-PHB                                                                                                                                                                                                                                                                                           | Configures the QoS policy for packets that match the class or classes.                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class IP-AF11                                                                                                                                                                                                                                                                                              | Associates the traffic class with the service policy.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 5 | <b>police</b> <i>bps</i> [ <i>burst-normal</i> ] [ <i>burst-max</i> ]<br><b>conform-action</b> <i>action</i> <b>exceed-action</b> <i>action</i><br>[ <b>violate-action</b> <i>action</i> ]<br><br><b>Example:</b><br>Router(config-p-map-c)# police 8000<br>conform-action<br>set-mpls-experimental-imposition-transmit 4<br>exceed-action<br>set-mpls-experimental-imposition-transmit 2 | Configures the Traffic Policing feature, including the following: <ul style="list-style-type: none"> <li>• Action to take on packets that conform to the rate limit specified in the SLA.</li> <li>• Action to take on packets that exceed the rate limit specified in the SLA.</li> </ul> At the <i>action</i> field, enter <b>set-mpls-experimental-imposition</b> <i>value</i> , where <i>value</i> is the value to which the MPLS EXP field will be set. |

|        | Command or Action                                                                                                         | Purpose                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                   | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 7 | <b>service-policy input</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy input<br>set-MPLS-PHB | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                         |

## Ingress PE Router—P Facing Interface

This procedure classifies packets based on their MPLS EXP field and provides appropriate discard and scheduling treatments.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
6. **random-detect**
7. **interface** *type slot/port*
8. **service-policy output** *name*

### DETAILED STEPS

|        | Command or Action                                                                                                                                | Purpose                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map MPLS-AF1                                                  | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                              |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental<br>topmost 2 4 | Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class. |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos                                                    | Configures the QoS policy for packets that match the class or classes.                                                                   |

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class MPLS-AF1                                                     | Associates the traffic class with the service policy.                                                                                                                                                             |
| Step 5 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }<br><br><b>Example:</b><br>Router(config-p-map-c)# bandwidth percent 40 | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.                                      |
| Step 6 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                              | Enables a WRED drop policy for a traffic class that has a bandwidth guarantee.                                                                                                                                    |
| Step 7 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                                           | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 8 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output-qos                                   | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                             |

## P Router—P Facing Interface

This procedure classifies packets based on their MPLS EXP field and provides appropriate discard and scheduling treatments.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
6. **random-detect**
7. **interface** *type slot/port*
8. **service-policy output** *name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map MPLS-AF1                                                   | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                                                       |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 2 4     | Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class.                                                                          |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos                                                     | Configures the QoS policy for packets that match the class or classes.                                                                                                                                            |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class MPLS-AF1                                                     | Associates the traffic class with the service policy.                                                                                                                                                             |
| Step 5 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }<br><br><b>Example:</b><br>Router(config-p-map-c)# bandwidth percent 40 | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.                                      |
| Step 6 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                              | Applies WRED to the policy based on the IP Precedence or the MPLS EXP field value.                                                                                                                                |
| Step 7 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                                           | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 8 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output output-qos                            | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                             |

## Egress PE Router—Customer Facing Interface

This procedure classifies a packet based on its IP DSCP value and provides appropriate discard and scheduling treatments.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match ip dscp** *dscp-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
6. **random-detect dscp-based**
7. **interface** *type slot/port*
8. **service-policy output** *name*

### DETAILED STEPS

|        | Command or Action                                                                                          | Purpose                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map IP-AF1              | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                  |
| Step 2 | <b>match ip dscp</b> <i>dscp-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match ip dscp 4 0  | Uses the DSCP values as the match criteria.                                                                                                                                  |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos              | Configures the QoS policy for packets that match the class or classes.                                                                                                       |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class AF1                   | Associates the traffic class with the service policy.                                                                                                                        |
| Step 5 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }                                 | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth. |
| Step 6 | <b>random-detect dscp-based</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect dscp-based | Enables a WRED drop policy for a traffic class that has a bandwidth guarantee.                                                                                               |

|        | Command or Action                                                                                                      | Purpose                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 8 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output output-qos | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                             |

## Configuring Uniform Mode

This section describes how to configure the following:

- [Ingress PE Router—Customer Facing Interface, page 32](#)
- [Ingress PE Router—P Facing Interface, page 34](#)
- [P Router—Upstream P Facing Interface, page 35](#)
- [P Router—Downstream P Facing Interface, page 36](#)
- [Egress PE Router—P Facing Interface, page 37](#)
- [Egress PE Router—Customer Facing Interface, page 38](#)

For examples, see the “Uniform Mode Configuration Example” section on page 44.



### Note

The steps that follow show one way, but not the only way, to configure Uniform mode.

## Ingress PE Router—Customer Facing Interface

This procedure configures a policy map to set the MPLS EXP field in imposed label entries.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match ip dscp** *dscp-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
6. **interface** *type slot/port*
7. **service-policy input** *name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>class-map</b> <i>class-name</i></p> <p><b>Example:</b><br/>Router(config)# class-map IP-AF11</p>                                                                                                                                                                                                                                                                                            | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <p><b>match ip dscp</b> <i>dscp-values</i></p> <p><b>Example:</b><br/>Router(config-c-map)# match ip dscp 4</p>                                                                                                                                                                                                                                                                                   | Uses the DSCP values as the match criteria.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <p><b>policy-map</b> <i>name</i></p> <p><b>Example:</b><br/>Router(config)# policy-map set-MPLS-PHB</p>                                                                                                                                                                                                                                                                                           | Configures the QoS policy for packets that match the class or classes.                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 4 | <p><b>class</b> <i>class-name</i></p> <p><b>Example:</b><br/>Router(config-p-map)# class IP-AF11</p>                                                                                                                                                                                                                                                                                              | Associates the traffic class with the service policy.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 5 | <p><b>police</b> <i>bps</i> [<i>burst-normal</i>] [<i>burst-max</i>]<br/><b>conform-action</b> <i>action</i> <b>exceed-action</b> <i>action</i><br/>[<b>violate-action</b> <i>action</i>]</p> <p><b>Example:</b><br/>Router(config-p-map-c)# police 8000<br/>conform-action<br/>set-mpls-experimental-imposition-transmit 3<br/>exceed-action<br/>set-mpls-experimental-imposition-transmit 2</p> | <p>Configures the Traffic Policing feature, including the following:</p> <ul style="list-style-type: none"> <li>Action to take on packets that conform to the rate limit specified in the SLA.</li> <li>Action to take on packets that exceed the rate limit specified in the SLA.</li> </ul> <p>At the <i>action</i> field, enter <b>set-mpls-experimental-imposition</b> <i>value</i>, where <i>value</i> is the value to which the MPLS EXP field will be set.</p> |
| Step 6 | <p><b>interface</b> <i>type slot/port</i></p> <p><b>Example:</b><br/>Router(config)# interface ethernet 3/0</p>                                                                                                                                                                                                                                                                                   | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number.                                                                                                                                                                                                                                                     |
| Step 7 | <p><b>service-policy input</b> <i>name</i></p> <p><b>Example:</b><br/>Router(config-if)# service-policy input<br/>set-MPLS-PHB</p>                                                                                                                                                                                                                                                                | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                                                                                                                                                                                                                                                                             |

## Ingress PE Router—P Facing Interface

This procedure classifies packets based on their MPLS EXP field and provides appropriate discard and scheduling treatments.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
6. **random-detect**
7. **interface** *type slot/port*
8. **service-policy output** *name*

### DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map MPLS-AF1                                               | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                  |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 2 3 | Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class.                                     |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map output-qos                                                 | Configures the QoS policy for packets that match the class or classes.                                                                                                       |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class MPLS-AF1                                                 | Associates the traffic class with the service policy.                                                                                                                        |
| Step 5 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }                                                                    | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth. |
| Step 6 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                          | Enables a WRED drop policy for a traffic class that has a bandwidth guarantee.                                                                                               |

|        | Command or Action                                                                                               | Purpose                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0         | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 8 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output-qos | Attaches a QoS policy to an interface and specifies that policies should be applied on packets leaving the interface.                                                                                             |

## P Router—Upstream P Facing Interface

This procedure classifies a packet based on the MPLS EXP field and sets the QoS group ID.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **set qos-group mpls experimental topmost**
6. **interface** *type slot/port*
7. **service-policy input** *name*

### DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map mpls-in                                                | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                              |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 4 5 | Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class. |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map policy2                                                    | Configures the QoS policy for packets that match the class or classes.                                                                   |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class mpls-in                                                  | Associates the traffic class with the service policy.                                                                                    |

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>set qos-group mpls experimental topmost</pre> <p><b>Example:</b><br/>Router(config-p-map-c)# set qos-group mpls experimental topmost</p> | Copies the MPLS EXP topmost field value into the QoS group ID. For more information, refer to <i>Enhanced Packet Marking</i> , Release 12.2(13)T.                                                                 |
| Step 6 | <pre>interface type slot/port</pre> <p><b>Example:</b><br/>Router(config)# interface ethernet 3/0</p>                                         | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card number, and the backplane slot number. |
| Step 7 | <pre>service-policy input name</pre> <p><b>Example:</b><br/>Router(config-if)# service-policy input policy2</p>                               | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                         |

## P Router—Downstream P Facing Interface

This procedure matches packets based on their QoS ID and sets the MPLS EXP field in the topmost label header to the QoS group ID.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match qos-group** *qos-group-value*
3. **policy-map** *name*
4. **class** *class-name*
5. **set mpls experimental topmost qos-group**
6. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
7. **random-detect**
8. **interface** *type slot/port*
9. **service-policy output** *name*

### DETAILED STEPS

|        | Command or Action                                                                                             | Purpose                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Step 1 | <pre>class-map class-name</pre> <p><b>Example:</b><br/>Router(config)# class-map qos-group-out</p>            | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class. |
| Step 2 | <pre>match qos-group qos-group-value</pre> <p><b>Example:</b><br/>Router(config-c-map)# match qos-group 4</p> | Identifies a specified QoS group value as a match criterion.                                |

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map policy3                                                        | Configures the QoS policy for packets that match the class or classes.                                                                                                                                             |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class qos-group-out                                                | Associates the traffic class with the service policy.                                                                                                                                                              |
| Step 5 | <b>set mpls experimental topmost qos-group</b><br><br><b>Example:</b><br>Router(config-p-map-c)# set mpls experimental topmost qos-group          | Copies the QoS group ID into the MPLS EXP field of the topmost label header. For more information, refer to <i>Enhanced Packet Marking</i> , Release 12.2(13)T.                                                    |
| Step 6 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }<br><br><b>Example:</b><br>Router(config-p-map-c)# bandwidth percent 40 | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth.                                       |
| Step 7 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                              | Applies WRED to the policy based on the IP Precedence or the MPLS EXP field value.                                                                                                                                 |
| Step 8 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/1                                           | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card numbers, and the backplane slot number. |
| Step 9 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output policy3                               | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                          |

## Egress PE Router—P Facing Interface

This procedure classifies a packet based on the MPLS EXP field and sets the QoS group ID.

### SUMMARY STEPS

1. **class-map** *class-name*
2. **match mpls experimental topmost** *mpls-values*
3. **policy-map** *name*
4. **class** *class-name*
5. **set qos-group mpls experimental topmost**
6. **interface** *type slot/port*
7. **service-policy input** *name*

## DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map mpls-in                                                | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                                                        |
| Step 2 | <b>match mpls experimental topmost</b> <i>mpls-values</i><br><br><b>Example:</b><br>Router(config-c-map)# match mpls experimental topmost 4 5 | Specifies the MPLS EXP field values used as a match criteria against which packets are checked to determine if they belong to the class.                                                                           |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map foo                                                        | Configures the QoS policy for packets that match the class or classes.                                                                                                                                             |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class mpls-in                                                  | Associates the traffic class with the service policy.                                                                                                                                                              |
| Step 5 | <b>set qos-group mpls experimental topmost</b><br><br><b>Example:</b><br>Router(config-p-map)# set qos-group mpls experimental topmost        | Copies the MPLS EXP topmost field value into the QoS group ID. For more information, refer to <i>Enhanced Packet Marking</i> , Release 12.2(13)T.                                                                  |
| Step 6 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/0                                       | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card numbers, and the backplane slot number. |
| Step 7 | <b>service-policy input</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy input foo                                 | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                          |

## Egress PE Router—Customer Facing Interface

This procedure matches packets based on their QoS ID and sets the IP Precedence field to the QoS group ID.

## SUMMARY STEPS

1. **class-map** *class-name*
2. **match qos-group** *qos-group-value*
3. **policy-map** *name*
4. **class** *class-name*

5. **set precedence qos-group**
6. **bandwidth** { *bandwidth-kbps* | **percent percent** }
7. **random-detect**
8. **interface** *type slot/port*
9. **service-policy output name**

## DETAILED STEPS

|        | Command or Action                                                                                                                          | Purpose                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map qos-out                                             | Specifies the class-map to which packets will be mapped (matched). Creates a traffic class.                                                                                  |
| Step 2 | <b>match qos-group</b> <i>qos-group-value</i><br><br><b>Example:</b><br>Router(config-c-map)# match qos-group 4                            | Identifies a specified QoS group value as a match criterion.                                                                                                                 |
| Step 3 | <b>policy-map</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# policy-map foo-out                                                 | Configures the QoS policy for packets that match the class or classes.                                                                                                       |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-p-map)# class qos-out                                               | Associates the traffic class with the service policy.                                                                                                                        |
| Step 5 | <b>set precedence qos-group</b><br><br><b>Example:</b><br>Router(config-p-map-c)# set precedence qos-group                                 | Sets the Precedence value in the packet header. For more information, refer to <i>Enhanced Packet Marking</i> , Release 12.2(13)T.                                           |
| Step 6 | <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent percent</b> }<br><br><b>Example:</b><br>Router(config-p-map-c)# bandwidth percent 40 | Specifies the minimum bandwidth guarantee to a traffic class. You can specify the minimum bandwidth guarantee in kilobits per second or by percent of the overall bandwidth. |
| Step 7 | <b>random-detect</b><br><br><b>Example:</b><br>Router(config-p-map-c)# random-detect                                                       | Applies WRED to the policy based on the IP Precedence or the MPLS EXP field value.                                                                                           |

|        | Command or Action                                                                                                      | Purpose                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 3/1                | Configures an interface type for Cisco series 7200 and Cisco series 7500 routers. Specifies the type of interface to be configured, the port, connector, or interface card numbers, and the backplane slot number. |
| Step 9 | <b>service-policy output</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# service-policy output<br>foo-out | Attaches a QoS policy to an interface and specifies that policies should be applied on packets coming into the interface.                                                                                          |

## Verifying MPLS DiffServ Tunneling Mode Support

- On PE routers, the **show policy-map interface** command displays the discard-class-based WRED in the output.
- In Short Pipe mode, the **show policy-map interface** command looks for the **set mpls experimental imposition** command.

## Troubleshooting Tips

- The IP QoS marking should not change in the service provider's network.
- QoS statistics should indicate that packets were scheduled in the correct classes.

## Configuration Examples for MPLS DiffServ Tunneling Modes

This section provides the following configuration examples:

- [Pipe Mode with an Explicit NULL LSP Configuration Example, page 41](#)
- [Short Pipe Mode Configuration Example, page 43](#)
- [Uniform Mode Configuration Example, page 44](#)



### Note

- You can configure only one tunneling mode.
- The examples that follow show one way, but not the only way, to configure the tunneling modes.

## Pipe Mode with an Explicit NULL LSP Configuration Example

### Ingress CE Router—Customer Facing Interface

In this example, packets are matched to class-map IP-AF11. The DSCP value 4 is used as the match criterion to determine whether a packet belongs to that class. Packets that are conforming have their MPLS EXP field set to 4. Packets that are out-of-rate have their MPLS EXP field set to 2.

```
class-map IP-AF11
 match ip dscp 4

policy-map set-MPLS-PHB
 class IP-AF11
 police 8000 conform-action set-mpls-experimental-imposition-transmit 4 exceed-action
 set-mpls-experimental-imposition-transmit 2

interface ethernet 3/0
 service-policy input set-MPLS-PHB
```

### Ingress CE Router—PE Facing Interface

In this example, MPLS EXP 2 and 4 are matched to class-map MPLS-AF1. Packets that match that class have WRED and WFQ enabled.

```
class-map match-any MPLS-AF1
 match mpls experimental topmost 2 4
 match ip dscp 4

policy-map output-qos
 class MPLS-AF1
 bandwidth percent 40
 random-detect

interface ethernet 3/0
 service-policy output output-qos
 mpls ip encapsulate explicit-null
```

### Ingress PE Router—P Facing Interface

In this example, the default label swap behavior copies the received MPLS EXP field value to the output MPLS EXP field. Packets that have an MPLS EXP value of 2 and 4 are matched to class-map MPLS-AF1. Packets that match that class have WRED and WFQ enabled.

```
class-map MPLS-AF1
 match mpls experimental topmost 2 4

policy-map output-qos
 class MPLS-AF1
 bandwidth percent 40
 random-detect

interface ethernet 3/0
 service-policy output output-qos
```

**P Router—P Facing Interface**

In this example, packets that have an MPLS EXP value of 2 or 4 are matched to class-map MPLS-AF1. Packets that match that class have WRED and WFQ enabled.

```
class-map MPLS-AF1
 match mpls experimental topmost 2 4

policy-map output-qos
 class MPLS-AF1
 bandwidth percent 40
 random-detect

interface ethernet 3/0
 service-policy output output-qos
```

**Egress PE Router—P Facing Interface**

In this example, qos-group 1 and discard-class 1 must be set to indicate the packet's PHB. The qos-group and discard-class are used for QoS classification at the output interface.

```
class-map MPLS-AF11
 match mpls experimental topmost 4

class-map MPLS-AF12
 match mpls experimental topmost 2

policy-map set-PHB
 class MPLS-AF11
 set qos-group 1
 set discard-class 1

class MPLS-AF12
 set qos-group 1
 set discard-class 2

interface ethernet 3/0
 service-policy input set-PHB
```

**Egress PE Router—Customer Facing Interface**

In this example, packets that have a qos-group value of 1 are matched to class-map Local-AF1. Packets that match that class have WRED based on their discard class value applied.

**Note**

You must issue the **mpls ip** command on this interface to receive packets with an explicit-NULL label from the CE router. The **mpls ip** command is not configured on the CE router's interface connected to this interface and therefore no LDP nor other label distribution protocol sessions will be established on this link.

```
class-map Local-AF1
 match qos-group 1

policy-map output-qos
 class Local-AF1
 bandwidth percent 40
 random-detect discard-class-based

interface ethernet 3/0
 mpls ip
 service-policy output output-qos
```

## Short Pipe Mode Configuration Example

**Note**

Short Pipe mode is not configured on CE routers.

**Ingress PE Router—Customer Facing Interface**

In this example, IP packets are matched to class-map IP-AF11. Packets that are conforming have their MPLS EXP field set to 4. Packets that are out-of-rate have their MPLS EXP field set to 2.

```
class-map IP-AF11
 match ip dscp 4

policy-map set-MPLS-PHB
 class IP-AF11
 police 8000 conform-action set-mpls-experimental-imposition-transmit 4 exceed-action
 set-mpls-experimental-imposition-transmit 2

interface ethernet 3/0
 service-policy input set-MPLS-PHB
```

**Ingress PE Router—P Facing Interface**

In this example, MPLS EXP 2 and 4 are matched to class-map MPLS-AF1. Packets that match that class have WRED and WFQ enabled.

```
class-map MPLS-AF1
 match mpls experimental topmost 2 4

policy-map output-qos
 class MPLS-AF1
 bandwidth percent 40
 random-detect

interface ethernet 3/0
 service-policy output output-qos
```

**P Router—P Facing Interface**

In this example, MPLS EXP 2 and 4 are matched to class-map MPLS-AF1. Packets that match that class have WRED and WFQ enabled.

```
class-map MPLS-AF1
 match mpls experimental topmost 2 4

policy-map output-qos
 class MPLS-AF1
 bandwidth percent 40
 random-detect

interface ethernet 3/0
 service-policy output output-qos
```

**Egress PE Router—Customer Facing Interface**

In this example, the egress PE router transmits IP packets. Packets are matched to class-map IP-AF1. Packets that match that class have WRED and WFQ enabled.

```
class-map IP-AF1
 match ip dscp 4 0

policy-map output-qos
 class AF1
 bandwidth percent 40
 random-detect dscp-based

interface ethernet 3/0
 service-policy output output-qos
```

## Uniform Mode Configuration Example

**Ingress PE Router—Customer Facing Interface**

In this example, IP packets are matched to class-map IP-AF11. Packets that are conforming have their MPLS EXP field set to 3. Packets that are out-of-rate have their MPLS EXP field set to 2.

```
class-map IP-AF11
 match ip dscp 4

policy-map set-MPLS-PHB
 class IP-AF11
 police 8000 conform-action set-mpls-experimental-imposition-transmit 3 exceed-action
 set-mpls-experimental-imposition-transmit 2

interface ethernet 3/0
 service-policy input set-MPLS-PHB
```

**Ingress PE Router—P Facing Interface**

In this example, MPLS EXP 2 and 3 are matched to class-map MPLS-AF1. Packets that match that class have WRED and WFQ enabled.

```
class-map MPLS-AF1
 match mpls experimental topmost 2 3

policy-map output-qos
 class MPLS-AF1
 bandwidth percent 40
 random-detect

interface ethernet 3/0
 service-policy output output-qos
```

### P Router—Upstream P Facing Interface

At the penultimate P router's input interface where the IGP label is popped, the EXP field value in the IGP label is copied to the QoS group ID. Suppose the MPLS EXP field value in the IGP label was recolored in the core to 4 or 5. In this example, MPLS EXP values 4 and 5 are matched to class-map mpls-in. For packets that match that class, the MPLS EXP value in the IGP label is copied to the QoS group ID.

```
class-map mpls-in
 match mpls experimental topmost 4 5

policy-map policy2
 class mpls-in
 set qos-group mpls experimental topmost

interface ethernet 3/0
 service-policy input policy2
```

### P Router—Downstream P Facing Interface

In this example, QoS group IDs 4 and 5 are matched to class-map qos-group-out. For packets that match that class, the MPLS EXP field in the topmost outgoing label is set to the QoS group ID.

```
class-map qos-group-out
 match qos-group 4
 match qos-group 5

policy-map policy3
 class qos-group-out
 set mpls experimental topmost qos-group
 bandwidth percent 40
 random-detect

interface ethernet 3/1
 service-policy output policy3
```

### Egress PE Router—P Facing Interface

In this example, packets with MPLS EXP values 4 or 5 are matched to class-map mpls-in. The EXP field value from the label header is copied to the QoS group ID.

```
class-map mpls-in
 match mpls experimental topmost 4 5

policy-map foo
 class mpls-in
 set qos-group mpls experimental topmost

interface ethernet 3/0
 service-policy input foo
```

**Egress PE Router—Customer Facing Interface**

In this example, the egress PE router transmits IP packets. QoS group IDs 4 and 5 are matched into class-map qos-out and the IP Precedence field of those packets is set to the QoS group ID.

```
class-map qos-out
 match qos-group 4
 match qos-group 5

policy-map foo-out
 class qos-out
 set precedence qos-group
 bandwidth percent 40
 random-detect

interface ethernet 3/1
 service-policy output foo-out
```

## Additional References

The following sections provide additional references related to MPLS DiffServ Tunneling Modes:

- [Related Documents, page 46](#)
- [Standards, page 47](#)
- [MIBs, page 47](#)
- [RFCs, page 47](#)
- [Technical Assistance, page 48](#)

## Related Documents

| Related Topic            | Document Title                                                                                                                                                                                                                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiffServ                 | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Switching Services Command Reference</a>, Release 12.2</li> <li>• <a href="#">Cisco IOS Terminal Services Configuration Guide</a>, Release 12.2</li> <li>• <a href="#">MPLS Class of Service Enhancements</a>, Release 12.1(5)T</li> </ul>            |
| MPLS Traffic Engineering | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Switching Services Command Reference</a>, Release 12.2</li> <li>• <a href="#">Cisco IOS Terminal Services Configuration Guide</a>, Release 12.2</li> <li>• <a href="#">Diff-Serv-aware MPLS Traffic Engineering</a>, Release 12.2(4)T</li> </ul>      |
| QoS                      | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>, Release 12.2</li> <li>• <a href="#">Cisco IOS Quality of Service Solutions Configuration Guide</a>, Release 12.2</li> <li>• <a href="#">Enhanced Packet Marking</a>, Release 12.2(13)T</li> </ul> |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs                                                   | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **match discard-class**
- **match mpls experimental topmost**
- **match qos-group**
- **mpls ip encapsulate explicit-null**
- **police**
- **random-detect discard-class**
- **random-detect discard-class-based**
- **set discard-class**
- **set mpls experimental imposition**
- **set mpls experimental topmost**
- **set qos-group**

## Glossary

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

**class**—Classifies traffic, such as voice. You define a traffic class with the **class-map** command.

**class-map**—Defines what you want to match in a packet. For example, a class-map may specify voice packets.

**core**—The MPLS network. At the edges, there are edge routers.

**customer network**—A network that is under the control of an end customer. A customer network can use private addresses as defined in RFC 1918. Customer networks are logically isolated from each other and from the service provider's network.

**DiffServ**—Application-level QoS and traffic management in an architecture that incorporates mechanisms to control bandwidth, delay, jitter, and packet loss. Application traffic can be categorized into multiple classes (aggregates), with QoS parameters defined for each class. A typical arrangement would be to categorize traffic into premium, gold, silver, bronze, and best-effort classes.

**DSCP**—differentiated services code point, or DiffServ code point. A marker in the header of each IP packet that prompts network routers to apply differentiated grades of service to various packet streams. The value in the IP header indicates which PHB is to be applied to the packet.

**discard-class**—Local variable used to indicate the discard profile.

**E-LSP**—An LSP in which the QoS of a packet is determined solely by the MPLS EXP field in the MPLS header. E-LSPs are not supported by ATM-LSRs.

**edge router**—A router that is at the edge of the network. It defines the boundary of the MPLS network. It receives and transmits packets. Also referred to as edge label switch router and label edge router.

**egress router**—Router at the edge of the network where packets are leaving.

**encapsulation**—The wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit.

**explicit null label**—A label that just has an EXP value. A value of zero (0) represents the explicit NULL label. This label can only be at the bottom of the label stack. It indicates that the label stack must be popped, and the forwarding of the packet must then be based on the IPv4 header. Sometimes there may be requirements to have a label in the stack when no label is required. If you want to retain the MPLS EXP field to the next hop, you use an explicit null.

**ingress router**—Router at the edge of the network where packets are being received by the network.

**IP Precedence field**—The first three bits in the header of IP packets. These bits allow you to specify the QoS for an IP packet.

**L-LSP**—An LSP where a particular mechanism of implementing QoS using DiffServ is used. An LSP in which routers infer the QoS treatment for MPLS packets from the packet label and the EXP bits (or the CLP bit for cell-mode MPLS). The label is used to encode the class to which a packet belongs and the MPLS EXP field (or the CLP bit for cell-mode MPLS) is used to encode the drop precedence of the packet.

**LSR**—A router that is part of the MPLS network. An LSR forwards a packet based on the value of a label encapsulated in the packet.

**label**—A short, fixed-length label that tells switching nodes how to forward data (packets). MPLS associates a label with each route. A label associates a network address with the output interface onto which the packet should be transmitted. In the MPLS network, the next-hop IGP (Interior Gateway Protocol) router always advertises to the preceding IGP router (the upstream router) what label should be placed on the packets. The next-hop BGP (Border Gateway Protocol) router always advertises to the preceding BGP router what label should be placed on the packets.

**label disposition**—The act of removing the last MPLS label from a packet.

**label entry**—A label entry contains a label value (which includes labels and other information for forwarding the packet) and an MPLS EXP field (which pertains to the QoS of the packet). When there are two label entries, the top label entry is the IGP (Interior Gateway Protocol) label. The bottom label entry is the BGP (Border Gateway Protocol) label.

**label imposition**—The act of putting MPLS labels onto a packet for transmission on a label switched path (LSP).

**layer management**—Ability to apply an additional layer of PHB marking to a packet.

**MPLS**—Multiprotocol Label Switching. Emerging industry standard upon which label switching is based.

**MPLS EXP field**—In an MPLS entry, the per-hop behavior (PHB) is marked in the MPLS EXP field within the MPLS label entry.

**P router**—provider core router.

**PE router**—provider edge router. A router, at the edge of a service provider's network, that interfaces to CE routers.

**penultimate hop popping**—Removing a label at the penultimate router. A label is removed and copied to the label that is one lower.

**penultimate router**—The second-to-last router; that is, the router that is immediately before the egress router.

**PHB**—per-hop behavior. A unique discard and scheduling behavior that is applied to a packet. The DiffServ treatment (scheduling/dropping) applied by a router to all the packets that are to experience the same DiffServ service.

**policing**—Limiting the input or output transmission rate of a class of traffic based on user-defined criteria. Policing marks packets by setting the IP precedence value, the qos-group, or the DSCP value.

**policy map**—Action that is taken if a packet matches what was specified in the class-map. For example, if voice packets were identified and the class-map and voice packets are received, the specified policy map action is taken.

**pop**—The act of removing a label entry from a packet.

**provider network**—A backbone network that is under the control of a service provider, and provides transport between customer sites.

**push**—To put a label entry onto a packet.

**QoS**—quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

**QoS transparency**—Method of forwarding packets through a network where the customer's IP marking in the IP packet is preserved.

**qos-group**—Local variable that indicates the PHB scheduling class (PSC).

**rate limiting**—See *policing*.

**recolor**—To change the PHB marking on a packet.

**swap**—To replace a label entry on a packet.

**ToS**—type of service. Byte in the IPv4 header.

**traffic policy**—A traffic policy consists of a traffic class and one or more QoS features. You create a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).

**transparency**—Preservation of the customer's IP marking in the IP packet.

**tunneling**—The ability of QoS to be transparent from one edge of a network to the other edge of the network.

**VPN**—Virtual Private Network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**WRED**—weighted random early detection. A queuing method that ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

**Note**

---

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels

---

**First Published:**12.0(14)ST

**Last Updated:** February 28, 2006

The MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels feature provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load.

## History for the MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels Feature

| Release    | Modification                                                   |
|------------|----------------------------------------------------------------|
| 12.0(14)ST | This feature was introduced.                                   |
| 12.2(4)T   | This feature was integrated into Release 12.2(4)T.             |
| 12.2(4)T2  | Support for the Cisco 7500 series routers was added.           |
| 12.2(14)S  | This feature was integrated into Cisco IOS Release 12.2(14)S.  |
| 12.2(28)SB | This feature was integrated into Cisco IOS Release 12.2(28)SB. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Feature Overview, page 2](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 8](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)

## Feature Overview

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically (for example, once per day) adjusts the tunnel's allocated bandwidth to be the largest sample for the tunnel since the last adjustment.

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

## Benefits

The automatic bandwidth feature makes it easy to configure and monitor the bandwidth for Multiprotocol Label Switching (MPLS) traffic engineering tunnels. If automatic bandwidth is configured for a tunnel, traffic engineering automatically adjusts the the tunnel's bandwidth.

## Restrictions

The automatic bandwidth adjustment feature treats each tunnel for which it has been enabled independently. That is, it adjusts the bandwidth for each such tunnel according to the adjustment frequency configured for the tunnel and the sampled output rate for the tunnel since the last adjustment without regard for any adjustments previously made or pending for other tunnels.

## Related Features and Technologies

The automatic bandwidth feature is related to:

- MPLS traffic engineering
- Resource Reservation Protocol (RSVP)

## Prerequisites

Your network must support the following:

- MPLS traffic engineering tunnels
- IP Cisco Express Forwarding

## Configuration Tasks

Perform the following tasks before you enable automatic bandwidth adjustment:

- Configure MPLS tunnels.
- Configure Cisco Express Forwarding.

Perform the following tasks to configure automatic bandwidth adjustment:

- [Configuring a Platform to Support Traffic Engineering Tunnels, page 3](#)
- [Configuring IS-IS for MPLS Traffic Engineering, page 4](#)
- [Configuring OSPF for MPLS Traffic Engineering, page 4](#)
- [Configuring an MPLS Traffic Engineering Tunnel, page 5](#)
- [Configuring Bandwidth on Each Link That the Tunnels Cross, page 6](#)
- [Configuring a Platform to Support Automatic Bandwidth Adjustment, page 6](#)
- [Configuring Automatic Bandwidth Adjustment for a Tunnel, page 7](#)
- [Configuring the Interval for Computing Tunnel Average Output Rate, page 7](#)

## Configuring a Platform to Support Traffic Engineering Tunnels

To configure a platform to support traffic engineering tunnels, perform the following steps in configuration mode:

|        | Command                                         | Purpose                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>ip cef</b>                   | Enables standard Cisco Express Forwarding operation.<br><br>For information about Cisco Express Forwarding configuration and the command syntax, see <a href="#">Cisco Express Forwarding Overview</a> in the <i>Cisco IOS IP Switching Configuration Guide</i> and see the <a href="#">Cisco IOS Switching Command Reference</a> . |
| Step 2 | Router(config)# <b>mpls traffic-eng tunnels</b> | Enables the MPLS traffic engineering tunnel feature on a device.                                                                                                                                                                                                                                                                    |

## Configuring IS-IS for MPLS Traffic Engineering

To configure Intermediate System-to-Intermediate System (IS-IS) for MPLS traffic engineering, perform the steps described below. For a description of the IS-IS commands, see the [Cisco IOS IP Routing Protocols Command Reference](#).

|               | Command                                                            | Purpose                                                                                                                      |
|---------------|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router isis</b>                                 | Enables IS-IS routing and specifies an IS-IS process for IP. This command places you in router configuration mode.           |
| <b>Step 2</b> | Router(config-router)# <b>mpls traffic-eng level-1</b>             | Turns on MPLS traffic engineering for IS-IS level 1.                                                                         |
| <b>Step 3</b> | Router(config-router)# <b>mpls traffic-eng router-id loopback0</b> | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0. |
| <b>Step 4</b> | Router(config-router)# <b>metric-style wide</b>                    | Configures a router to generate and accept only new-style type, length, value objects (TLVs).                                |

## Configuring OSPF for MPLS Traffic Engineering

To configure Open Shortest Path First (OSPF) for MPLS traffic engineering, perform the steps described below. For a description of the OSPF commands, see the [Cisco IOS IP Routing Protocols Command Reference](#).

|               | Command                                                            | Purpose                                                                                                                                                                                                                                                                                                       |
|---------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf process-id</b>                      | Configures an OSPF routing process for IP. You are placed in router configuration mode.<br><br>The <i>process-id</i> is an internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process. |
| <b>Step 2</b> | Router(config-router)# <b>mpls traffic-eng area 0</b>              | Turns on MPLS traffic engineering for OSPF area 0.                                                                                                                                                                                                                                                            |
| <b>Step 3</b> | Router(config-router)# <b>mpls traffic-eng router-id loopback0</b> | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0.                                                                                                                                                                                  |

## Configuring an MPLS Traffic Engineering Tunnel

To configure an MPLS traffic engineering tunnel, perform these steps in interface configuration mode. This tunnel has two path setup options: a preferred explicit path and a backup dynamic path. For more detailed descriptions of the commands and their arguments, see the [Cisco IOS Multiprotocol Label Switching Command Reference](#).

.k

|        | Command                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <i>tunnel-interface</i>                                                                                                                                               | Configures an interface type and enters interface configuration mode.                                                                                                                                                                                                       |
| Step 2 | Router(config-if)# <b>ip unnumbered loopback0</b>                                                                                                                                                      | Gives the tunnel interface an IP address.<br><br>An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.                                                                                                             |
| Step 3 | Router(config-if)# <b>tunnel destination</b> <i>A.B.C.D</i>                                                                                                                                            | Specifies the destination for a tunnel. The destination must be the MPLS traffic engineering router ID of the destination device.                                                                                                                                           |
| Step 4 | Router(config-if)# <b>tunnel mode mpls traffic-eng</b>                                                                                                                                                 | Sets the tunnel encapsulation mode to MPLS traffic engineering.                                                                                                                                                                                                             |
| Step 5 | Router(config-if)# <b>tunnel mpls traffic-eng bandwidth</b> <i>bandwidth</i>                                                                                                                           | Configures the bandwidth for the MPLS traffic engineering tunnel. If automatic bandwidth is configured for the tunnel, the <b>tunnel mpls traffic-eng bandwidth</b> command configures the initial tunnel bandwidth, which will be adjusted by the autobandwidth mechanism. |
| Step 6 | Router(config-if)# <b>tunnel mpls traffic-eng path-option</b> <i>number</i><br>{ <b>dynamic</b>   <b>explicit</b> { <b>name</b> <i>path-name</i>   <b>id</b> <i>path-number</i> }} [ <b>lockdown</b> ] | Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database. A dynamic path is used if an explicit path is currently unavailable.                                                                 |

## Configuring Bandwidth on Each Link That the Tunnels Cross

To configure bandwidth on each link that the tunnels cross, perform the following steps:

|        | Command                                                                                                                      | Purpose                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config-if)# <b>mpls traffic-eng tunnels</b>                                                                           | Enables MPLS traffic engineering tunnels on an interface.                                                                                                          |
| Step 2 | Router(config-if)# <b>ip rsvp bandwidth</b> <i>interface-kbps</i><br><i>single-flow-kbps</i> [ <b>sub-pool</b> <i>kbps</i> ] | Enables RSVP for IP on an interface and specifies the amount of interface bandwidth (in kbps) allocated for RSVP flows (for example, traffic engineering tunnels). |

## Configuring a Platform to Support Automatic Bandwidth Adjustment

To enable automatic bandwidth adjustment on a platform and initiate sampling the output rate for tunnels configured for bandwidth adjustment, enter the following global configuration command:

| Command                                                                         | Description                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config)# <b>mpls traffic-eng auto-bw timers frequency</b> [ <i>sec</i> ] | Enables automatic bandwidth adjustment on a platform and begins sampling the output rate for tunnels that have been configured for automatic bandwidth adjustment. The <i>sec</i> option can be used to specify the sampling interval, in seconds. |

To disable automatic bandwidth adjustment on a platform, use the **no** version of the command, which terminates output rate sampling and bandwidth adjustment for tunnels. In addition, the **no** form of the command restores the configured bandwidth for each tunnel where “configured bandwidth” is determined as follows:

- If the tunnel bandwidth was explicitly configured via the **tunnel mpls traffic-eng bandwidth** command after the running configuration was written (if at all) to the startup configuration, the “configured bandwidth” is the bandwidth specified by that command.
- Otherwise, the “configured bandwidth” is the bandwidth specified for the tunnel in the startup configuration.

## Configuring Automatic Bandwidth Adjustment for a Tunnel

To enable automatic bandwidth adjustment for a tunnel and constrain the range of automatic bandwidth adjustments applied to the tunnel, perform these steps in interface configuration mode:

|        | Command                                                                                                                | Purpose                                                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <i>tunnel-interface</i>                                                               | Configures an interface type and enters interface configuration mode.                                                                                                                                        |
| Step 2 | Router(config-if)# <b>tunnel mpls traffic-eng auto-bw</b><br><b>max-bw</b> <i>seconds</i> <b>min-bw</b> <i>seconds</i> | Enables automatic bandwidth adjustment for the tunnel. Specifies the minimum and maximum automatic bandwidth allocations, in kilobits per second, that can be applied to the tunnel by automatic adjustment. |

## Configuring the Interval for Computing Tunnel Average Output Rate

To specify the interval for computing the average output rate for an MPLS traffic engineering tunnel, use the **load-interval** command shown below.

| Command                                                  | Purpose                                                                                       |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Router(config)# <b>interface</b> <i>tunnel-interface</i> | Configures an interface type and enters interface configuration mode.                         |
| Router(config-if)# <b>load-interval</b> <i>sec</i>       | Configures the interval over which the input and output rates for the interface are averaged. |

## Verifying the Configuration

To verify that automatic bandwidth has been configured, enter the command shown below. For a detailed description of the command, see the [Cisco IOS Multiprotocol Label Switching Command Reference](#).

| Command                                                                         | Purpose                                                                                                               |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Router(config)# <b>show mpls traffic-eng tunnels</b><br><i>tunnel-interface</i> | Shows information about tunnels, including automatic bandwidth information for tunnels that have the feature enabled. |

Example:

The following is sample output from the **show mpls traffic-eng tunnels** command. In the command output:

- The auto-bw line indicates that automatic bandwidth adjustment is enabled for the tunnel.
- 86400 is the time, in seconds, between bandwidth adjustments.
- 85477 is the time, in seconds, remaining until the next bandwidth adjustment.
- 5347 is the largest bandwidth sample since the last bandwidth adjustment.
- 5000 is the last bandwidth adjustment and the bandwidth currently requested for the tunnel.

```

Router# show mpls traffic-eng tunnels

Name:tagsw4500-9_t1 (Tunnel1) Destination:10.0.0.11
Status:
 Admin:up Oper:up Path:valid Signalling:connected

 path option 1, type explicit pbr_south (Basis for Setup, path weight 30)
 path option 2, type dynamic

Config Parameters:
 Bandwidth:5000 kbps (Global) Priority:7 7 Affinity:0x0/0xFFFF
 AutoRoute: disabled LockDown:disabled Loadshare:5000 bw-based
 auto-bw:(86400/85477) 5347 Bandwidth Requested:5000

```

## Troubleshooting Tips

Each **tunnel mpls traffic-eng auto-bw** command supersedes the previous one. Therefore, if you want to specify multiple options for a tunnel, you must specify them all in a single **tunnel mpls traffic-eng auto-bw** command.

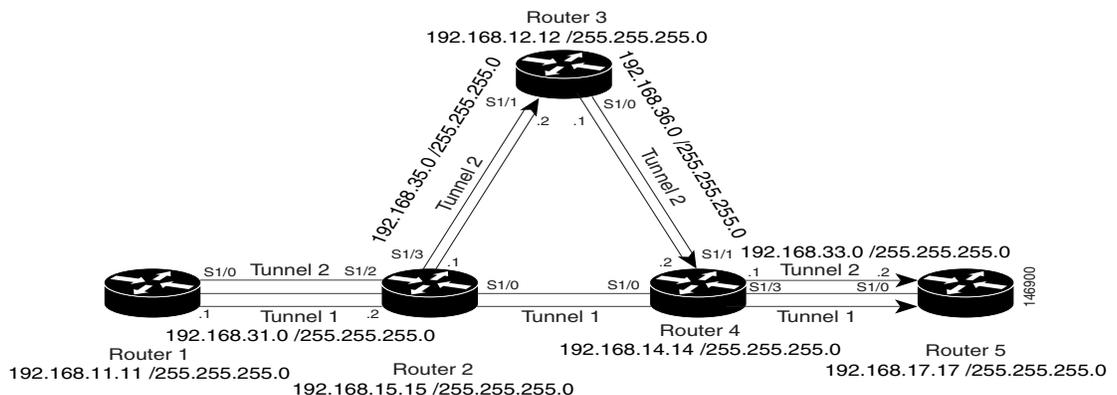
## Configuration Examples

This section provides the following configuration examples:

- [MPLS Traffic Engineering Configuration for Automatic Bandwidth, page 9](#)
- [Tunnel Configuration for Automatic Bandwidth, page 9](#)

Figure 1 illustrates a sample MPLS topology. The next sections contain sample configuration commands to configure automatic bandwidth adjustment for MPLS traffic engineering tunnels originating on Router 1 and to enable it for Tunnel1. The examples omit some configuration required for MPLS traffic engineering, such as the required RSVP and Interior Gateway Protocol (IGP) (IS-IS or OSPF) configuration, because the purpose of these examples is to illustrate the configuration for automatic bandwidth adjustment. For information about configuring MPLS traffic engineering see the *Cisco IOS Switching Services Configuration Guide*.

**Figure 1** Sample MPLS Traffic Engineering Tunnel Configuration



## MPLS Traffic Engineering Configuration for Automatic Bandwidth

The following illustrates how to use the **mpls traffic-eng auto-bw timers** command to enable automatic bandwidth adjustment for Router 1. The command specifies that the output rate is to be sampled every 10 minutes for tunnels configured for automatic bandwidth.

```
ip cef
mpls traffic-eng tunnels
mpls traffic-eng auto-bw timers frequency 600 !Enable automatic bandwidth adjustment
interface loopback 0
ip address 192.168.11.11 255.255.255.0
```

## Tunnel Configuration for Automatic Bandwidth

The following example illustrates how to use the **tunnel mpls traffic-eng auto-bw** command to enable automatic bandwidth adjustment for Tunnel1. The command specifies a maximum allowable bandwidth of 2000 kbps, a minimum allowable bandwidth of 1000 kbps, and that the default automatic bandwidth adjustment frequency of once a day be used.

```
interface tunnel1
 ip unnumbered loopback 0
 tunnel destination 192.168.17.17 255.255.255.0
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng auto bw max-bw 2000 min-bw 1000 !Enable automatic bandwidth
 !adjustment for Tunnel1
```

## Additional References

The following sections provide references related to MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels.

## Related Documents

| Related Topic                              | Document Title                                                   |
|--------------------------------------------|------------------------------------------------------------------|
| IP command                                 | <i>Cisco IOS IP Switching Command Reference</i>                  |
| Quality of service solutions commands      | <i>Cisco IOS Quality of Service Solutions Command Reference</i>  |
| Quality of service solutions configuration | <i>Quality of Service Overview</i>                               |
| Multiprotocol Label Switching commands     | <i>Cisco IOS Multiprotocol Label Switching Command Reference</i> |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB                          | MIBs Link                                                                                                                                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html).

For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **clear mpls traffic-eng auto-bw timers**
- **mpls traffic-eng auto-bw timers**
- **tunnel mpls traffic-eng auto-bw**

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

---

**First Published: January 16, 2003**

**Last Updated: February 7, 2006**

The MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion feature provides a means to exclude a link or node from the path for an Multiprotocol Label Switching (MPLS) TE label-switched path (LSP).

The feature is enabled through the **ip explicit-path** command that allows you to create an IP explicit path and enter a configuration submode for specifying the path. The feature adds to the submode commands the **exclude-address** command for specifying addresses to exclude from the path.

If the excluded address for an MPLS TE LSP identifies a flooded link, the constraint-based shortest path first (CSPF) routing algorithm does not consider that link when computing paths for the LSP. If the excluded address specifies a flooded MPLS TE router ID, the CSPF routing algorithm does not allow paths for the LSP to traverse the node identified by the router ID.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS Traffic Engineering \(TE\)—IP Explicit Address Exclusion”](#) section on page 9.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for MPLS Traffic Engineering \(TE\)—IP Explicit Address Exclusion, page 2](#)
- [Restrictions for MPLS Traffic Engineering \(TE\)—IP Explicit Address Exclusion, page 2](#)
- [Information About MPLS Traffic Engineering \(TE\)—IP Explicit Address Exclusion, page 2](#)
- [How to Configure MPLS Traffic Engineering \(TE\)—IP Explicit Address Exclusion, page 3](#)
- [Configuration Examples for MPLS Traffic Engineering \(TE\)—IP Explicit Address Exclusion, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Glossary, page 9](#)
- [Feature Information for MPLS Traffic Engineering \(TE\)—IP Explicit Address Exclusion, page 9](#)

## Prerequisites for MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

Your network must support the following Cisco IOS features in order to support IP explicit address exclusion:

- MPLS
- IP Cisco Express Forwarding
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)

## Restrictions for MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

MPLS TE will accept an IP explicit path comprised of either all excluded addresses configured by the **exclude-address** command or all included addresses configured by the **next-address** command, but not a combination of both.

## Information About MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

To configure the MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion feature, you need to understand the following concepts:

- [MPLS Traffic Engineering, page 3](#)
- [Cisco Express Forwarding, page 3](#)

## MPLS Traffic Engineering

MPLS is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

Traffic engineering (TE) is the process of adjusting bandwidth allocations to ensure that enough is left for high-priority traffic.

In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream, then fixes the bandwidth available for that tunnel.

## Cisco Express Forwarding

Cisco Express Forwarding is an advanced, Layer 3 switching technology inside a router. It defines the fastest method by which a Cisco router forwards packets from ingress to egress interfaces. The **ip cef** command enables Cisco Express Forwarding globally, and the **ip route-cache cef** command enables Cisco Express Forwarding on an interface.

# How to Configure MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

This section contains the following procedures:

- [Configuring IP Explicit Address Exclusion](#) (required)
- [Configuring an MPLS Traffic Engineering Tunnel](#) (required)

## Configuring IP Explicit Address Exclusion

To configure IP Explicit Address Exclusion, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip explicit-path {name *path-name* | identifier *number*} [enable | disable]**
4. **exclude-address *ip-address***
5. **exit**
6. **show ip explicit-path**

## DETAILED STEPS

|        | Command                                                                                                                                                                                       | Purpose                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                | Enters global configuration mode.                                                                                                                               |
| Step 3 | <b>ip explicit-path</b> {name <i>path-name</i>   <b>identifier</b> <i>number</i> } [ <b>enable</b>   <b>disable</b> ]<br><br><b>Example:</b><br>Router(config)# ip explicit-path name OmitR12 | Specifies the name or number of the explicit path, and enables the path. Enters explicit-path configuration mode.                                               |
| Step 4 | <b>exclude-address</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(cfg-ip-expl-path)# exclude-address 10.12.12.12                                                                      | Excludes the specified link or node from consideration by the constraint-based SPF.<br><br>The <i>ip-address</i> is a link address or the router ID for a node. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(cfg-ip-expl-path)# exit                                                                                                                          | Exits from explicit-path configuration mode. Returns to global configuration mode.                                                                              |
| Step 6 | <b>show ip explicit-path</b><br><br><b>Example:</b><br>Router# show ip explicit-path                                                                                                          | Displays information about configured IP explicit paths.                                                                                                        |

## Configuring an MPLS Traffic Engineering Tunnel

To configure an MPLS traffic engineering tunnel, perform the following steps.

## SUMMARY STEPS

- enable**
- configure terminal**
- interface** *type number*
- ip unnumbered loopback0**
- tunnel destination** *ip-address*
- tunnel mode mpls traffic-eng**
- tunnel mpls traffic-eng bandwidth** *bandwidth*

8. `tunnel mpls traffic-eng path-option` *number* { `dynamic` | `explicit` { `name` *path-name* | `ID` *path-number* } } [`lockdown`]
9. `exit`
10. `show mpls traffic eng tunnels`

## DETAILED STEPS

|        | Command                                                                                                                                                    | Purpose                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><code>enable</code></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                    | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                |
| Step 2 | <p><code>configure terminal</code></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                               | <p>Enters global configuration mode.</p>                                                                                                                                 |
| Step 3 | <p><code>interface</code> <i>type number</i></p> <p><b>Example:</b><br/>Router(config)# interface tunnel11</p>                                             | <p>Configures an interface type and enters interface configuration mode.</p>                                                                                             |
| Step 4 | <p><code>ip unnumbered loopback0</code></p> <p><b>Example:</b><br/>Router(config-if)# ip unnumbered loopback0</p>                                          | <p>Assigns the tunnel interface an IP address.</p> <p>An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.</p> |
| Step 5 | <p><code>tunnel destination</code> <i>ip-address</i></p> <p><b>Example:</b><br/>Router(config-if)# tunnel destination 10.11.11.11</p>                      | <p>Specifies the destination for a tunnel.</p> <p>The destination of the tunnel must be the MPLS traffic engineering router ID of the destination device.</p>            |
| Step 6 | <p><code>tunnel mode mpls traffic-eng</code></p> <p><b>Example:</b><br/>Router(config-if)# tunnel mode mpls traffic-eng</p>                                | <p>Sets the tunnel encapsulation mode to MPLS traffic engineering.</p>                                                                                                   |
| Step 7 | <p><code>tunnel mpls traffic-eng bandwidth</code> <i>bandwidth</i></p> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng bandwidth 100</p> | <p>Configures the bandwidth for the MPLS traffic engineering tunnel.</p>                                                                                                 |

|         | Command                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <pre>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   ID path-number}} [lockdown]</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng path-option 2 dynamic</p> | <p>Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.</p> <p>A dynamic path is used if an explicit path is unavailable.</p> <p><b>Note</b> To configure a path option that specifies an exclude address, specify the <b>explicit</b> keyword (not the <b>dynamic</b> keyword) and specify an IP explicit path configured according to the steps in the “<a href="#">Configuring IP Explicit Address Exclusion</a>” section.</p> |
| Step 9  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                                                                                                                  | Exits from interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 10 | <pre>show mpls traffic eng tunnels</pre> <p><b>Example:</b><br/>Router# show mpls traffic eng tunnels</p>                                                                                                           | Shows information about tunnels, including the current tunnel path if a tunnel is operational. By viewing the command output, you can determine the path that was used to build a tunnel. If you entered the <b>exclude-address</b> command, the specified link or node should not be listed.                                                                                                                                                                                                                       |

## Configuration Examples for MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

This section includes the following configuration examples:

- [Configuring IP Explicit Address Exclusion: Example, page 6](#)
- [Configuring an MPLS Traffic Engineering Tunnel: Example, page 7](#)

### Configuring IP Explicit Address Exclusion: Example

The following example shows how to configure an MPLS TE tunnel with two path options: a preferred explicit path with an excluded address and a backup dynamic path.

Configure the IP explicit path named OmitR12, which excludes the router with router ID 10.12.12.12:

```
ip explicit-path name OmitR12
exclude-address 10.12.12.12
Explicit Path name OmitR12:
```

```
1: exclude-address 10.12.12.12
exit
```

To verify the configuration of the explicit path, use the **show ip explicit-path** command.

```
show ip explicit-paths name OmitR12
PATH OmitR12 (loose source route, path complete, generation 3)
1: exclude-address 10.12.12.12
```

**Note**

You must know the router IDs for LSRs (nodes) in the network; in this example, that 10.12.12.12 is a router ID. Otherwise, it will not be apparent whether the specified address is the IP address of a link or a router ID.

## Configuring an MPLS Traffic Engineering Tunnel: Example

The following example configures Tunnel11 with its two options, where the preferred path option is the IP explicit path OmitR2:

```
interface tunnel11
ip unnumbered loopback0
tunnel destination 10.11.11.11
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name OmitR12
tunnel mpls traffic-eng path-option 2 dynamic
```

**Note**

There are additional commands for configuring properties for TE tunnels such as bandwidth and priority. For descriptions of those commands, refer to the *Cisco IOS Switching Services Configuration Guide*.

## Additional References

The following sections provide references related to the MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion feature.

## Related Documents

| Related Topic | Document Title                                                                  |
|---------------|---------------------------------------------------------------------------------|
| MPLS commands | <i>Cisco IOS Multiprotocol Label Switching Command Reference</i> , Release 12.4 |

## Standards

| Standard                                                    | Title |
|-------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature. | —     |

## MIBs

| MIB                                                    | MIBs Link |
|--------------------------------------------------------|-----------|
| No new or modified MIBs are supported by this feature. | —         |

## RFCs

| RFC                                                    | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **exclude-address**

# Glossary

**CEF**—Cisco express forwarding. A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

**IP explicit path**—A list of IP addresses, each representing a node or link in the explicit path.

**link**—Network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

**MPLS**—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**node**—Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.



**Note**

---

See *Internetworking Terms and Acronyms* for terms not included in this glossary.

---

## Feature Information for MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



**Note**

---

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---

**Table 1** Feature Information for MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

| Feature Name                                                | Releases                                                                    | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion | 12.0(14)ST<br>12.2(4)T<br>12.2(4)T2<br>12.2(14)S<br>12.0(32)S<br>12.2(28)SB | <p>The MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion feature provides a means to exclude a link or node from the path for an Multiprotocol Label Switching (MPLS) TE label-switched path (LSP).</p> <p>The following command was introduced by this feature:<br/><b>exclude-address.</b></p> <p>In 12.0(14)ST, this feature was introduced.</p> <p>In 12.2(4)T, this feature was integrated into Release 12.2(4)T.</p> <p>In 12.2(4)T2, this feature was integrated into Release 12.2(4)T2.</p> <p>In 12.2(14)S, this feature was integrated into Release 12.2(14)S.</p> <p>In 12.0(32)S, this feature was integrated into Release 12.0(32)S.</p> <p>In 12.2(28)SB, this feature was integrated into Release 12.2(28)SB.</p> |

isco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; Cisco Business Registrars, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Speed, and WebEx are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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 with Cisco and any other company. (0709R)

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering MIB

---

**First Published: May 22, 2001**

**Last Updated: November 1, 2006**

The MPLS Traffic Engineering MIB enables Simple Network Management Protocol (SNMP) agent support in Cisco IOS software for Multiprotocol Label Switching (MPLS) traffic engineering (TE) management, as implemented in the MPLS Traffic Engineering MIB (MPLS TE MIB). The SNMP agent code operating in conjunction with the MPLS TE MIB enables a standardized, SNMP-based approach to be used in managing the MPLS TE features in Cisco IOS software.

## **Finding Feature Information in This Module**

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for the MPLS Traffic Engineering MIB](#)” section on page 15.*

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Information About the MPLS Traffic Engineering MIB, page 2](#)
- [Restrictions for the MPLS Traffic Engineering MIB, page 4](#)
- [How to Configure the MPLS Traffic Engineering MIB, page 10](#)
- [Configuration Examples for the MPLS Traffic Engineering MIB, page 12](#)
- [Additional References, page 13](#)
- [Command Reference, page 14](#)
- [Feature Information for the MPLS Traffic Engineering MIB, page 15](#)
- [Glossary, page 16](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Information About the MPLS Traffic Engineering MIB

This section describes the following:

- [MPLS Traffic Engineering MIB Cisco Implementation, page 2](#)
- [Capabilities Supported by the MPLS Traffic Engineering MIB, page 2](#)
- [Notification Generation Events, page 3](#)
- [Notification Implementation, page 3](#)
- [Benefits of MPLS Traffic Engineering MIB, page 4](#)
- [MPLS Traffic Engineering MIB Layer Structure, page 4](#)

## MPLS Traffic Engineering MIB Cisco Implementation

The MPLS TE MIB is based on the Internet Engineering Task Force (IETF) draft MIB entitled *draft-ietf-mpls-te-mib-05.txt*, which includes objects describing features that support MPLS TE. This IETF draft MIB is revised occasionally and is becoming a standard. Accordingly, Cisco's implementation of the MPLS TE MIB is expected to track the evolution of the IETF draft MIB.

Slight differences between the IETF draft MIB and the implementation of the TE capabilities within Cisco IOS software require some minor translations between the MPLS TE MIB and the internal data structures of Cisco IOS software. These translations are made by the SNMP agent code that is installed and operating on various hosts within the network. This SNMP agent code, running in the background as a low priority process, provides a management interface to Cisco IOS software.

The SNMP objects defined in the MPLS TE MIB can be displayed by any standard SNMP utility. All MPLS TE MIB objects are based on the IETF draft MIB; thus, no specific Cisco SNMP application is required to support the functions and operations pertaining to the MPLS TE MIB.

## MPLS Traffic Engineering Overview

MPLS TE capabilities in Cisco IOS software enable an MPLS backbone to replicate and expand upon the TE capabilities of Layer 2 ATM and Frame Relay networks.

TE capabilities are essential to effective management of service provider and Internet service provider (ISP) backbones. Such backbones must support high transmission capacities, and the networks incorporating backbones must be extremely resilient to link or node failures.

The MPLS TE facilities built into Cisco IOS software provide a feature-rich, integrated approach to managing the large volumes of traffic that typically flow through WANs. The MPLS TE facilities are integrated into Layer 3 network services, thereby optimizing the routing of IP traffic in the face of constraints imposed by existing backbone transmission capacities and network topologies.

## Capabilities Supported by the MPLS Traffic Engineering MIB

The following functionality is supported in the MPLS Traffic Engineering MIB:

- The ability to generate and queue notification messages that signal changes in the operational status of MPLS TE tunnels.
- Extensions to existing SNMP commands that provide the ability to enable, disable, and configure notification messages for MPLS TE tunnels.

- The ability to specify the name or the IP address of a network management station (NMS) in the operating environment to which notification messages are to be sent.
- The ability to write notification configurations into nonvolatile memory.

## Notification Generation Events

When MPLS TE notifications are enabled (see the **snmp-server enable traps (mpls)** command), notification messages relating to specific events within Cisco IOS software are generated and sent to a specified NMS in the network.

For example, an `mplsTunnelUp` notification is sent to an NMS when an MPLS TE tunnel is configured and the tunnel transitions from an operationally “down” state to an “up” state.

Conversely, an `mplsTunnelDown` notification is generated and sent to an NMS when an MPLS TE tunnel transitions from an operationally “up” state to a “down” state.

Finally, an `mplstunnelRerouted` notification is sent to the NMS under the following conditions:

- The signaling path of an existing MPLS TE tunnel fails for some reason and a new path option is signaled and placed into effect (that is, the tunnel is rerouted).
- The signaling path of an existing MPLS TE tunnel is fully operational, but a better path option can be signaled and placed into effect (that is, the tunnel can be reoptimized). This reoptimization can be triggered by:
  - A timer
  - The issuance of an **mpls traffic-eng reoptimize** command
  - A configuration change that requires the resignaling of a tunnel

Path options are configurable parameters that you can use to specify the order of priority for establishing a new tunnel path. For example, you can create a tunnel head configuration and define any one of many path options numbered 1 through x, with “1” being the highest priority option and “x” being an unlimited number of lower priority path options. Thus, there is no limit to the number of path options that you can specify in this manner.

## Notification Implementation

When an MPLS TE tunnel interface (or any other device interface, such as an Ethernet or Packet over SONET (POS) interface) transitions between an up and down state, an Interfaces MIB (ifMIB) link notification is generated. When such a notification occurs in an MPLS TE MIB environment, the interface is checked by software to determine if the notification is associated with an MPLS TE tunnel. If so, the interfaces MIB link notification is interlinked with the appropriate `mplsTunnelUp` or `mplsTunnelDown` notification to provide notification to the NMS regarding the operational event occurring on the tunnel interface. Hence, the generation of an Interfaces MIB link notification pertaining to an MPLS traffic engineering tunnel interface begets an appropriate `mplsTunnelUp` or `mplsTunnelDown` notification that is transmitted to the specified NMS.

An `mplsTunnelRerouted` notification is generated whenever the signaling path for an MPLS TE tunnel changes. However, software intelligence in the MPLS TE MIB prevents the reroute notification from being sent to the NMS when a TE tunnel transitions between an up or down state during an administrative or operational status check of the tunnel. Either an up/down notification or a reroute notification can be sent in this instance, but not both. This action prevents unnecessary traffic on the network.

## Benefits of MPLS Traffic Engineering MIB

The MPLS Traffic Engineering MIB provides the following benefits:

- Provides a standards-based SNMP interface for retrieving information about MPLS TE.
- Provides information about the traffic flows on MPLS TE tunnels.
- Presents MPLS TE tunnel routes, including the configured route, the Interior Gateway Protocol (IGP) calculated route, and the actual route traversed.
- Provides information, in conjunction with the Interfaces MIB, about how a tunnel was rerouted in the event of a link failure.
- Provides information about the configured resources used for an MPLS TE tunnel.
- Supports the generation and queueing of notifications that call attention to major changes in the operational status of MPLS TE tunnels; forwards notification messages to a designated NMS for evaluation or action by network administrators.

## MPLS Traffic Engineering MIB Layer Structure

The SNMP agent code supporting the MPLS TE MIB follows the existing model for such code in Cisco IOS software and is, in part, generated by the Cisco IOS tool set, based on the MIB source code.

The SNMP agent code, which has a layered structure similar to that of the MIB support code in Cisco IOS software, consists of four layers:

- Platform independent layer—This layer is generated primarily by the Cisco IOS MIB development tool set and incorporates platform and implementation independent functions. The Cisco IOS MIB development tool set creates a standard set of files associated with a MIB.
- Application interface layer—The functions, names, and template code for MIB objects in this layer are also generated by the Cisco IOS MIB development tool set.
- Application specific layer—This layer provides an interface between the application interface layer and the application program interface (API) and data structures layer and performs tasks needed to retrieve required information from Cisco IOS software, such as searching through data structures.
- API and data structures layer—This layer contains the data structures or APIs within Cisco IOS software that are retrieved or called in order to set or retrieve SNMP management information.

## Restrictions for the MPLS Traffic Engineering MIB

The following restrictions apply to the MPLS TE MIB for Cisco IOS releases:

- Supports read-only (RO) permission for MIB objects.
- Contains no configuration support by means of SET functions, except for the `mplsTunnelTrapEnable` object (which has been made writable). Accordingly, the MPLS TE MIB contains indexing support for the Interfaces MIB.
- Supports only SNMP GET, GETNEXT, and GETBULK retrieval functions, except in the case of the `mplsTunnelTrapEnable` object (which has been made writable by means of SET functions).
- Contains no support for Guaranteed Bandwidth Traffic Engineering (GBTE) or Auto Bandwidth features.

## Features and Technologies Related to MPLS Traffic Engineering MIB

The MPLS TE MIB feature is used in conjunction with the following:

- Standards-based SNMP network management application
- MPLS
- MPLS TE
- MPLS label switching router MIB (MPLS-LSR-MIB)

## Supported Objects in the MPLS Traffic Engineering MIB

The MPLS TE MIB contains numerous tables and object definitions that provide read-only SNMP management support for the MPLS TE features in Cisco IOS software. The MPLS TE MIB conforms to Abstract Syntax Notation One (ASN.1), thus reflecting an idealized MPLS TE database.

Using any standard SNMP network management application, you can retrieve and display information from the MPLS TE MIB by using GET operations; similarly, you can traverse information in the MIB database for display by using GETNEXT operations.

The MPLS TE MIB tables and objects supported in Cisco IOS releases follow. Important MIB tables (those highlighted in bold type) are described briefly in accompanying text.

- `mplsTunnelConfigured`—Total number of tunnel configurations that are defined on this node.
- `mplsTunnelActive`—Total number of label-switched paths (LSPs) that are defined on this node.
- `mplsTunnelTEDistProto`—The IGP distribution protocol in use.
- `mplsTunnelMaxHops`—The maximum number of hops any given tunnel can utilize.
- `mplsTunnelIndexNext`—Unsupported; set to 0.
- **`mplsTunnelTable`**—Entries in this table with an instance of 0 and a source address of 0 represent tunnel head configurations. All other entries in this table represent instances of LSPs, both signaled and standby. If a tunnel instance is signaled, its operating status (`operStatus`) is set to “up” (1) and its instance corresponds to an active LSP.

Tunnel configurations exist only on the tunnel head where the tunnel interface is defined. LSPs traverse the network and involve tunnel heads, tunnel midpoints, and tunnel tails.

Pointers in the tunnel table refer to corresponding entries in other MIB tables. By using these pointers, you can find an entry in the `mplsTunnelTable` and follow a pointer to other tables for additional information. The pointers are the following: *`mplsTunnelResourcePointer`*, *`mplsTunnelHopTableIndex`*, *`mplsTunnelARHopTableIndex`*, and *`mplsTunnelCHopTableIndex`*.

The tunnel table is indexed by tunnel ID, tunnel instance, tunnel source address, and tunnel destination address. The description of each entry has an alphabetic suffix (a), (b), or (c), if appropriate, to indicate the applicability of the entry

- a. For tunnel head configurations only
- b. For LSPs only
- c. For both tunnel head configurations and LSPs

Following is a list and description of each entry.

- `mplsTunnelIndex`—Same as tunnel ID (c).
- `mplsTunnelInstance`—Tunnel instance of the LSP; 0 for head configurations (b).

- mplsTunnelIngressLSRId—Source IP address of the LSP; 0 for head configurations (b).
- mplsTunnelEgressLSRId—Destination IP address of the tunnel (c).
- mplsTunnelName—Command name for the tunnel interfaces (a).
- mplsTunnelDescr—Descriptive name for tunnel configurations and LSPs (c).
- mplsTunnelIsIf—Indicator of whether the entry represents an interface (c).
- mplsTunnelIfIndex—Index of the tunnel interface within the ifMIB (a).
- mplsTunnelXCPointer—(For midpoints only – no tails) Pointer for the LSP within the mplsXCTable of the MPLS LSR MIB (b).
- mplsTunnelSignallingProto—Signaling protocol used by tunnels (c).
- mplsTunnelSetupPrio—Setup priority of the tunnel (c).
- mplsTunnelHoldingPrio—Holding priority of the tunnel (c).
- mplsTunnelSessionAttributes—Session attributes (c).
- mplsTunnelOwner—Tunnel owner (c).
- mplsTunnelLocalProtectInUse—Not implemented (c).
- mplsTunnelResourcePointer—Pointer into the Resource Table (b).
- mplsTunnelInstancePriority—Not implemented (b).
- mplsTunnelHopTableIndex—Index into the Hop Table (a).
- mplsTunnelARHopTableIndex—Index into the AR Hop Table (b).
- mplsTunnelCHopTableIndex—Index into the C Hop Table (b).
- mplsTunnelPrimaryTimeUp—Amount of time, in seconds, that the current path has been up (a).
- mplsTunnelPathChanges—Number of times a tunnel has been resignalled (a).
- mplsTunnelLastPathChange—Amount of time, in seconds, since the last path resignaling occurred (a).
- mplsTunnelCreationTime—Time stamp when the tunnel was created (a).
- mplsTunnelStateTransitions—Number of times the tunnel has changed state (a).
- mplsTunnelIncludeAnyAffinity—Not implemented (a).
- mplsTunnelIncludeAllAffinity—Attribute bits that must be set for the tunnel to traverse a link (a).
- mplsTunnelExcludeAllAffinity—Attribute bits that must *not* be set for the tunnel to traverse a link (a).
- mplsTunnelPathInUse—Path option number being used for the tunnel’s path. If no path option is active, this object will be 0 (a).
- mplsTunnelRole—Role of the tunnel on the router; that is, head, midpoint, or tail (c).
- mplsTunneltotalUptime—Amount of time, in seconds, that the tunnel has been operationally up (a).
- mplsTunnelInstanceUptime—Not implemented (b).
- mplsTunnelAdminStatus—Administrative status of a tunnel (c).
- mplsTunnelOperStatus—Actual operating status of a tunnel (c).
- mplsTunnelRowStatus—This object is used in conjunction with configuring a new tunnel. This object will always be seen as “active” (a).

- `mplsTunnelStorageType`—Storage type of a tunnel entry (c).
- `mplsTunnelHopListIndexNext`—Next valid index to use as an index in the `mplsTunnelHopTable`.
- **`mplsTunnelHopTable`**—Entries in this table exist only for tunnel configurations and correspond to the path options defined for the tunnel. Two types of path options exist: *explicit* and *dynamic*. This table shows all hops listed in the explicit path options, while showing only the destination hop for dynamic path options. The tunnel hop table is indexed by tunnel ID, path option, and hop number.

Following is a list and description of each table entry.

- `mplsTunnelHopListIndex`—Primary index into the table.
- `mplsTunnelHopIndex`—Secondary index into the table.
- `mplsTunnelHopAddrType`—Indicates if the address of this hop is the type IPv4 or IPv6.
- `mplsTunnelHopIpv4Addr`—The IPv4 address of this hop.
- `mplsTunnelHopIpv4PrefixLen`—The prefix length of the IPv4 address.
- `mplsTunnelHopIpv6Addr`—The IPv6 address of this hop.
- `mplsTunnelHopIpv6PrefixLen`—The prefix length of the IPv6 address.
- `mplsTunnelHopAsNumber`—This object will contain 0 or the AS number of the hop, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelHopLspId`—This object will contain 0 or the LSPID of the tunnel, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelHopType`—Denotes whether this tunnel hop is routed in a strict or loose fashion.
- `mplsTunnelHopRowStatus`—This object is used in conjunction with the configuring of a new row in the table.
- `mplsTunnelHopStorageType`—The storage type of this MIB object.
- `mplsTunnelResourceIndexNext`
- **`mplsTunnelResourceTable`**—Entries in this table correspond to the “Tspec” information displayed when you execute the **show mpls traffic-eng tunnels** command. These entries exist only for LSPs.

The tunnel resource table is indexed by address and hop number. Following the *mplsTunnelResourcePointer* pointer from the tunnel table is the best way to retrieve information from this table.

Following is a list and description of each table entry.

- `mplsTunnelResourceIndex`—The primary index into this table.
- `mplsTunnelResourceMaxRate`—The maximum rate, in bits per second, supported by this tunnel.
- `mplsTunnelResourceMeanRate`—The mean rate, in bits per second, supported by this tunnel.
- `mplsTunnelResourceMaxBurstSize`—The maximum burst size, in bytes, allowed by this tunnel.
- `mplsTunnelResourceRowStatus`—This object is used in conjunction with the configuration of a new row in the table.
- `mplsTunnelResourceStorageType`—The storage type of this MIB object.
- **`mplsTunnelARHopTable`**—Entries in this table correspond to the actual route taken by the tunnel, and whose route was successfully signaled by the network. The hops present in this table correspond to those present in the record route object (RRO) in Resource Reservation Protocol (RSVP). You can also display the information in this table by executing the **show mpls traffic-eng tunnels** command.

The actual route hop table is indexed by address and hop number. Following the *mplsTunnelARHopTableIndex* pointer from the tunnel table is the best way to retrieve information from this table. The entries in the table are listed and described below.

Following is a list and description of each table entry.

- *mplsTunnelARHopListIndex*—The primary index into this table.
- *mplsTunnelARHopIndex*—The secondary index into this table.
- *mplsTunnelARHopIpv4Addr*—The IPv4 address of this hop.
- *mplsTunnelARHopIpv4PrefixLen*—The prefix length of the IPv4 address.
- *mplsTunnelARHopIpv6Addr*—The IPv6 address of this hop.
- *mplsTunnelARHopIpv6PrefixLen*—The prefix length of the IPv6 address.
- *mplsTunnelARHopAsNumber*—This object will contain 0 or the AS number of the hop, depending on the value of *mplsTunnelARHopAddrType*.
- *mplsTunnelARHopAddrType*—The type of address for this MIB entry, either IPv4 or IPv6.
- *mplsTunnelARHopType*—Denotes whether this tunnel hop is routed in a strict or loose manner.
- ***mplsTunnelCHopTable***—Entries in this table correspond to the explicit route object (ERO) in RSVP, which is used to signal the LSP. The list of hops in this table will contain those hops that are computed by the constraint-based shortest path first (SPF) algorithm. In those cases where “loose” hops are specified for the tunnel, this table will contain the hops that are “filled-in” between the loose hops to complete the path. If you specify a complete explicit path, the computed hop table matches your specified path.

The computed hop table is indexed by address and hop number. Following the *mplsTunnelCHopTableIndex* pointer from the tunnel table is the best way to retrieve information from this table. The entries in the table are listed and described below.

- *mplsTunnelCHopListIndex*—The primary index into this table.
- *mplsTunnelCHopIndex*—The secondary index into this table.
- *mplsTunnelCHopAddrType*—Indicates if the address of this hop is the type IPv4 or IPv6.
- *mplsTunnelCHopIpv4Addr*—The IPv4 address of this hop.
- *mplsTunnelCHopIpv4PrefixLen*—The prefix length of the IPv4 address.
- *mplsTunnelCHopIpv6Addr*—The IPv6 address of this hop.
- *mplsTunnelCHopIpv6PrefixLen*—The prefix length of the IPv6 address.
- *mplsTunnelCHopAsNumber*—This object will contain 0 or the AS number of the hop, depending on the value of *mplsTunnelHopAddrType*.
- *mplsTunnelCHopType*—Denotes whether this tunnel hop is routed in a strict or loose way.
- ***mplsTunnelPerfTable***—The tunnel performance table, which augments the ***mplsTunnelTable***, provides packet and byte counters for each tunnel. This table contains the following packet and byte counters:
  - *mplsTunnelPerfPackets*—This packet counter works only for tunnel heads.
  - *mplsTunnelPerfHCPackets*—This packet counter works only for tunnel heads.
  - *mplsTunnelPerfErrors*—This packet counter works only for tunnel heads.
  - *mplsTunnelPerfBytes*—This byte counter works for tunnel heads and tunnel midpoints, but not for tunnel tails.

- `mplsTunnelPerfHCBytes`—This byte counter works for tunnel heads and tunnel midpoints, but not for tunnel tails.
- `mplsTunnelTrapEnable`—The object type `mplsTunnelTrapEnable` is enhanced to be writable. Accordingly, if this object type is set to “TRUE,” the following notifications are enabled, thus giving you the ability to monitor changes in the operational status of MPLS TE tunnels:
  - `mplsTunnelUp`
  - `mplsTunnelDown`
  - `mplsTunnelRerouted`

If the `mplsTunnelTrapEnable` object is set to “FALSE,” such operational status notifications are not generated. These notification functions are based on the definitions (`mplsTeNotifications`) contained in the IEFT draft document entitled *draft-ietf-mpls-te-mib-05.txt*.

## CLI Access to MPLS Traffic Engineering MIB Information

Figure 1 shows commands that you can use to retrieve information from specific tables in the MPLS TE MIB. As noted in this figure, some information in the MPLS TE MIB is not retrievable by commands.

**Figure 1**      **Commands for Retrieving MPLS TE MIB Information**



### Retrieving Information from the MPLS Traffic Engineering MIB

This section describes how to efficiently retrieve information about TE tunnels. Such information can be useful in large networks that contain many TE tunnels.

Traverse across a single column of the *mplsTunnelTable*, such as *mplsTunnelName*. This action provides the indexes of every tunnel configuration, and any LSPs involving the host router. Using these indexes, you can perform a GET operation to retrieve information from any column and row of the *mplsTunnelTable*.

The *mplsTunnelTable* provides pointers to other tables for each tunnel. The column *mplsTunnelResourcePointer*, for example, provides an object ID (OID) that you can use to access resource allocation information in the *mplsTunnelResourceTable*. The columns *mplsTunnelHopTableIndex*, *mplsTunnelARHopTableIndex*, and *mplsTunnelCHopTableIndex* provide the primary index into the *mplsTunnelHopTable*, *mplsTunnelARHopTable*, and *mplsTunnelCHopTable*, respectively. By traversing the MPLS TE MIB in this manner using a hop table column and primary index, you can retrieve information pertaining to the hops of that tunnel configuration.

Because tunnels are treated as interfaces, the tunnel table column (*mplsTunnelIfIndex*) provides an index into the Interfaces MIB that you can use to retrieve interface-specific information about a tunnel.

## How to Configure the MPLS Traffic Engineering MIB

This section contains the following tasks:

- [Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router, page 10](#) (required)
- [Verifying the Status of the SNMP Agent, page 11](#) (optional)

### Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router

The SNMP agent for the MPLS TE MIB is disabled by default. To enable the SNMP agent for the MPLS TE MIB, perform the following steps.

#### SUMMARY STEPS

1. **telnet** *host*
2. **enable**
3. **show running-config**
4. **configure terminal**
5. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]
6. **snmp-server enable traps** [*identification-type*] [*notification-option*]
7. **exit**
8. **write memory**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>telnet host</code><br><br><b>Example:</b><br>Router> telnet 192.172.172.172                                                                                                    | Telnet to the router identified by the specified IP address (represented as <i>xxx.xxx.xxx.xxx</i> ).                                                                                                                                                                                                  |
| Step 2 | <code>enable</code><br><br><b>Example:</b><br>Router# enable                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                       |
| Step 3 | <code>show running-config</code><br><br><b>Example:</b><br>Router# show running-config                                                                                               | Displays the running configuration to determine if an SNMP agent is already running. <ul style="list-style-type: none"> <li>If no SNMP information is displayed, go to <a href="#">Step 5</a>. If any SNMP information is displayed, you can modify the information or change it as needed.</li> </ul> |
| Step 4 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                      |
| Step 5 | <code>snmp-server community string [view view-name] [ro   rw] [ipv6 nacl] [access-list-number]</code><br><br><b>Example:</b><br>Router(config)# snmp-server community comaccess ro 4 | Enables the read-only (RO) community string.                                                                                                                                                                                                                                                           |
| Step 6 | <code>snmp-server enable traps [identification-type] [notification-option]</code><br><br><b>Example:</b><br>Router(config)# snmp-server enable traps                                 | Enables an LSR to send SNMP notifications or informs to an SNMP host.<br><br><b>Note</b> This command is optional. After SNMP is enabled, all MIBs (not just the TE MIB) are available for the user to quer.                                                                                           |
| Step 7 | <code>exit</code><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                     | Exits global configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                   |
| Step 8 | <code>write memory</code><br><br><b>Example:</b><br>Router# write memory                                                                                                             | Writes the modified configuration to NVRAM, permanently saving the settings.                                                                                                                                                                                                                           |

## Verifying the Status of the SNMP Agent

To verify that the SNMP agent has been enabled on a host network device, perform the following steps.

**Step 1** `telnet host`

Use this command to Telnet to the target device:

```
Router# telnet 192.172.172.172
```

**Step 2 enable**

Use this command to enable SNMP on the target device:

```
Router# enable
```

**Step 3 show running-config**

Use this command to display the running configuration on the target device and examine the output for displayed SNMP information.

```
Router# show running-config
.
.
.
snmp-server community public ro
snmp-server community private ro
```

Any **snmp-server** statement that appears in the output and takes the form shown here verifies that SNMP has been enabled on that device.

---

## Configuration Examples for the MPLS Traffic Engineering MIB

This section contains the following configuration examples:

- [Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router: Example, page 12](#)

### Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router: Example

The following example shows how to enable an SNMP agent on a host network device:

```
Router# configure terminal
Router(config)# snmp-server community snmp-community-string
```

The following example shows how to enable SNMPv1 and SNMPv2C. The configuration permits any SNMP agent to access all MPLS TE MIB objects with read-only permissions using the community string *public*.

```
Router(config)# snmp-server community public
```

The following example shows how to allow read-only access to all MPLS TE MIB objects relating to members of access list 4 that specify the *comaccess* community string. No other SNMP agents will have access to any MPLS TE MIB objects.

```
Router(config)# snmp-server community comaccess ro 4
```

# Additional References

The following sections provide references related to the MPLS Traffic Engineering MIB.

## Related Documents

| Related Topic              | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS-based functionalities | <ul style="list-style-type: none"> <li>• <i>MPLS Label Distribution Protocol (LDP)</i></li> <li>• <i>MPLS Label Switching Router MIB</i></li> <li>• <i>MPLS Scalability Enhancements for the LSC LSR</i></li> <li>• <i>MPLS Scalability Enhancements for the ATM LSR</i></li> <li>• <i>MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for MPLS TE Tunnels</i></li> <li>• <i>MPLS Traffic Engineering (TE)—Scalability Enhancements</i></li> <li>• <i>MPLS Class of Service Enhancements</i></li> <li>• <i>RFC 2233 Interfaces MIB</i></li> </ul> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                           | MIBs Link                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS TE MIB<br>Interfaces MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                 |
|----------|---------------------------------------|
| RFC 2026 | <i>The Internet Standards Process</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **snmp-server community**
- **snmp-server enable traps (MPLS)**
- **snmp-server host**

# Feature Information for the MPLS Traffic Engineering MIB

Table 1 lists the release history for this MIB.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for the MPLS Traffic Engineering MIB

| Feature Name                 | Releases                                                                      | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering MIB | 12.0(17)S<br>12.0(17)ST<br>12.2(8)T<br>12.2(14)S<br>12.2(28)SB<br>12.2(31)SB2 | <p>The MPLS Traffic Engineering MIB feature enables the SNMP agent support in Cisco IOS software for MPLS TE management, as implemented in the MPLS TE MIB.</p> <p>In 12.0(17)S, this feature provided the ability to generate and queue SNMP notification messages that signal changes in the operational status of MPLS TE tunnels when you are using the MPLS TE MIB on Cisco 7500 series routers and Cisco 12000 series Internet routers.</p> <p>In 12.0(17)ST, support for SNMP traffic engineering notifications was extended to include Cisco 7500 series routers and Cisco 12000 series Internet routers.</p> <p>In 12.2(8)T, support for SNMP TE notifications was extended to include Cisco 7500 series routers. The <b>snmp-server host</b> command was modified.</p> <p>In 12.2(14)S, this feature was integrated.</p> <p>In 12.2(28)SB, this feature was integrated.</p> <p>In 12.2(31)SB2, this feature was integrated.</p> |
| MPLS Traffic Engineering MIB | Cisco IOS XE Release 2.1                                                      | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

# Glossary

**affinity bits**—An MPLS traffic engineering tunnel’s requirements on the attributes of the links it will cross. The tunnel’s affinity bits and affinity mask must match with the attributes of the various links carrying the tunnel.

**call admission precedence**—An MPLS traffic engineering tunnel with a higher priority will, if necessary, preempt an MPLS traffic engineering tunnel with a lower priority. An expected use is that tunnels that are harder to route will have a higher priority, and can preempt tunnels that are easier to route, on the assumption that those lower priority tunnels can find another path.

**constraint-based routing**—Procedures and protocols used to determine a route across a backbone taking into account resource requirements and resource availability, instead of simply using the shortest path.

**flow**—A traffic load entering the backbone at one point—point of presence (POP)—and leaving it from another that must be traffic engineered across the backbone. The traffic load will be carried across one or more LSP tunnels running from the entry POP to the exit POP.

**headend**—The LSR at which the tunnel originates. The tunnel’s “head” or tunnel interface will reside at this LSR as well.

**informs**—A type of notification message that is more reliable than a conventional trap notification message because an informs message requires acknowledgment.

**label**—A short, fixed-length data construct that tells switching nodes how to forward data (packets or cells).

**label-switched path (LSP) tunnel**—A configured connection between two routers, using label switching to carry the packets.

**LSP**—label-switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

**LSR**—label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MIB**—Management Information Base. A database of network management information (consisting of MIB objects) that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually by a GUI-based network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**notification** (see traps)—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred.

**NMS**—network management station. An NMS is a powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks.

**OSPF**—Open Shortest Path First. A link-state routing protocol used for routing IP.

**RSVP**—Resource Reservation Protocol. Protocol for reserving network resources to provide quality of service (QoS) guarantees to application flows.

**SNMP**—Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, manage configurations, collect statistics, monitor performance, and ensure network security.

**tailend**—The downstream, receive end of a tunnel.

**traffic engineering**—Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

**trap** (see notification)—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred. Traps (notifications) are less reliable than inform requests, because the receiver of the trap does not send an acknowledgment of receipt; furthermore, the sender of the trap cannot determine if the trap was received.

**VCI**—virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next network VCL as the cell passes through a series of ATM switches on its way to its final destination.

**VCC**—virtual channel connection. A VCC is a logical circuit consisting of VCLs that carries data between two endpoints in an ATM network. Sometimes called a virtual circuit connection.

**VCL**—virtual channel link. A VCL is the logical connection that exists between two adjacent switches in an ATM network.

**VPI**—virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next network VCL (see above) as the cell passes through a series of ATM switches on its way to its final destination.

**Note**

---

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

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.

© 2007 Cisco Systems, Inc. All rights reserved.





## **MPLS Virtual Private Networks**





# MPLS Layer 3 VPN Features Roadmap

---

This roadmap lists the features documented in the MPLS Layer 3 VPN configuration guide and maps them to the modules in which they appear.

## Roadmap History

This roadmap was first published on May 2, 2005, and last updated on May 2, 2005

## Feature and Release Support

[Table 1](#) lists MPLS VPN feature support for the following Cisco IOS software release trains:

- [Cisco IOS Release 12.0S](#)
- [Cisco IOS Release 12.2S](#)
- [Cisco IOS Releases 12.2T, 12.3, and 12.3T](#)

*Not all features may be supported in your Cisco IOS software release.*

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

---

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

**Table 1 Supported MPLS VPN Features**

| Release                        | Feature Name                                                     | Feature Description                                                                                                                                                                                                                                                                                                                                                                                                                          | Where Documented                                                                                                                                       |
|--------------------------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cisco IOS Release 12.0S</b> |                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                        |
| 12.0(29)S                      | MPLS VPN—Loadbalancing Support for Inter-AS and CSC VPNs         | This feature allows MPLS VPN Inter-AS and MPLS VPN CSC networks to load share traffic between adjacent LSRs that are connected by multiple links. The LSRs can be a pair of ASBRs or a CSC-PE and a CSC-CE. Using directly connected loopback peering allows load sharing at the IGP level, so more than one BGP session is not needed between the LSRs. No other label distribution mechanism is needed between the adjacent LSRs than BGP. | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                          |
| 12.0(27)S                      | eBGP Multipath                                                   | This feature installs multiple paths in the IP routing table when the eBGP paths are learned from a neighboring AS, instead of picking one best path.                                                                                                                                                                                                                                                                                        | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                          |
| 12.0(24)S                      | BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN | This feature allows multihomed autonomous systems and PE routers to be configured to distribute traffic across both eBGP and iBGP paths.                                                                                                                                                                                                                                                                                                     | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                          |
| 12.0(23)S                      | VRF Aware MPLS Static Labels                                     | This feature enable an MPLS VPN CSC network to use static labels at the edge of the VPN.                                                                                                                                                                                                                                                                                                                                                     | <a href="#">Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</a>                                                |
| 12.0(22)S                      | Inter-Autonomous Systems for MPLS VPNs                           | This feature enables an MPLS VPN to span service providers and autonomous systems. This feature explains how to configure the Inter-AS using the ASBRs to exchange VPNv4 Addresses.                                                                                                                                                                                                                                                          | <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a> |
|                                | MPLS VPN—Carrier Supporting Carrier                              | This feature enables you to create an MPLS VPN CSC network that uses LDP to transport MPLS labels and an IGP to transport routes.                                                                                                                                                                                                                                                                                                            | <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a>       |

**Table 1**      **Supported MPLS VPN Features (continued)**

| <b>Release</b>                 | <b>Feature Name</b>                                                | <b>Feature Description</b>                                                                                                                                                                                                   | <b>Where Documented</b>                                                                                                                                |
|--------------------------------|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(22)S<br>(cont.)           | MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution    | This feature enables you to create an MPLS VPN CSC network that uses BGP to transport routes and MPLS labels.                                                                                                                | <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a>                   |
|                                | MPLS Virtual Private Networks                                      | This feature allows a set of sites to be interconnected by means of an MPLS provider core network. At each customer site, one or more CE routers attach to one or more PE routers.                                           | <a href="#">Configuring MPLS Layer 3 VPNs</a>                                                                                                          |
|                                | MPLS VPN ID                                                        | This feature enables you to identify MPLS VPNs by a VPN identification number, as described in RFC 2685.                                                                                                                     | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                        |
|                                | MPLS VPN: Inter-AS — IPv4 BGP Label Distribution                   | This feature explains how to configure an MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the PE routers. Route reflectors exchange VPNv4 routes by using multihop, multiprotocol eBGP. | <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a> |
|                                | MPLS VPN—MIB Support                                               | This feature allows you to monitor and manage MPLS VPNs using MIBs.                                                                                                                                                          | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                         |
|                                | MPLS VPN — OSPF and Sham-Link Support                              | This feature allows you to configure a sham-link that directs traffic between VPN client sites over the MPLS VPN backbone.                                                                                                   | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                     |
|                                | MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge | This feature allows you to connect customers running EIGRP to an MPLS VPN.                                                                                                                                                   | <a href="#">Configuring MPLS Layer 3 VPNs</a>                                                                                                          |
|                                | MPLS VPN: VRF Selection Based on Source IP Address                 | This feature enables you to direct MPLS VPN traffic based on the source IP address of the packet.                                                                                                                            | <a href="#">Directing MPLS VPN Traffic Using a Source IP Address</a>                                                                                   |
| <b>Cisco IOS Release 12.2S</b> |                                                                    |                                                                                                                                                                                                                              |                                                                                                                                                        |
| 12.2(25)S                      | MPLS VPN—VRF Selection Using Policy Based Routing                  | This feature allows you to classify and forward VPN traffic based on match criteria, such as IP access lists, IP prefix lists, and packet length.                                                                            | <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a>                                                                                  |
| 12.2(18)S                      | MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge | This feature allows you to connect customers running EIGRP to an MPLS VPN.                                                                                                                                                   | <a href="#">Configuring MPLS Layer 3 VPNs</a>                                                                                                          |
|                                | MPLS VPN: VRF Selection Based on Source IP Address                 | This feature enables you to direct MPLS VPN traffic based on the source IP address of the packet.                                                                                                                            | <a href="#">Directing MPLS VPN Traffic Using a Source IP Address</a>                                                                                   |

**Table 1** Supported MPLS VPN Features (continued)

| Release   | Feature Name                                                    | Feature Description                                                                                                                                                                                                          | Where Documented                                                                                                                                       |
|-----------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(14)S | iBGP Multipath Load Sharing                                     | This feature enables the BGP speaking router to select multiple iBGP paths as the best paths to a destination.                                                                                                               | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                          |
|           | Inter-Autonomous Systems for MPLS VPNs                          | This feature enables an MPLS VPN to span service providers and autonomous systems. This feature explains how to configure the Inter-AS using the ASBRs to exchange VPNv4 Addresses.                                          | <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a> |
|           | MPLS Virtual Private Networks                                   | This feature allows a set of sites to be interconnected by means of an MPLS provider core network. At each customer site, one or more CE routers attach to one or more PE routers.                                           | <a href="#">Configuring MPLS Layer 3 VPNs</a>                                                                                                          |
|           | MPLS VPN—Carrier Supporting Carrier                             | This feature enables you to set up and create an MPLS VPN CSC network that uses LDP to transport MPLS labels and an IGP to transport routes.                                                                                 | <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a>       |
|           | MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution | This feature enables you to create an MPLS VPN CSC network that uses BGP to transport routes and MPLS labels.                                                                                                                | <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a>                   |
|           | MPLS VPN ID                                                     | This feature lets you identify MPLS VPNs by a VPN identification number, as described in RFC 2685.                                                                                                                           | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                        |
|           | MPLS VPN: Inter-AS—IPv4 BGP Label Distribution                  | This feature explains how to configure an MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the PE routers. Route reflectors exchange VPNv4 routes by using multihop, multiprotocol eBGP. | <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a> |
|           | MPLS VPN—MIB Support                                            | This feature allows you to monitor and manage MPLS VPNs using MIBs.                                                                                                                                                          | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                         |
|           | MPLS VPN—OSPF and Sham-Link Support                             | This feature allows you to configure a sham-link that directs traffic between VPN client sites over the MPLS VPN backbone.                                                                                                   | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                     |

**Table 1 Supported MPLS VPN Features (continued)**

| Release                                          | Feature Name                                                       | Feature Description                                                                                                                                                                                                         | Where Documented                                                                                                                                       |
|--------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cisco IOS Releases 12.2T, 12.3, and 12.3T</b> |                                                                    |                                                                                                                                                                                                                             |                                                                                                                                                        |
| 12.2(15)T                                        | MPLS VPN—MIB Support                                               | This feature allows you to monitor and manage MPLS VPNs using MIBs.                                                                                                                                                         | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                         |
|                                                  | MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge | This feature allows you to connect customers running EIGRP to an MPLS VPN.                                                                                                                                                  | <a href="#">Configuring MPLS Layer 3 VPNs</a>                                                                                                          |
| 12.2(13)T                                        | MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution    | This feature enables you to create an MPLS VPN CSC network that uses BGP to transport routes and MPLS labels.                                                                                                               | <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a>                   |
|                                                  | MPLS VPN: Inter-AS—IPv4 BGP Label Distribution                     | This feature enables you to configure an MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the PE routers. Route reflectors exchange VPNv4 routes by using multihop, multiprotocol eBGP. | <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a> |
| 12.3(7)T                                         | MPLS VPN—VRF Selection Using Policy Based Routing                  | This feature allows you to classify and forward VPN traffic based on match criteria, such as IP access lists, IP prefix lists, and packet length.                                                                           | <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a>                                                                                  |
| 12.3(6)                                          | MPLS VPN Half-Duplex VRF                                           | This feature allows you to configure an MPLS hub-and-spoke VPN that is more scalable than previously.                                                                                                                       | <a href="#">Configuring Scalable Hub-and-Spoke MPLS VPNs</a>                                                                                           |
| 12.2(8)T                                         | Dialer Map VRF-Aware for an MPLS VPN                               | This feature enables dialer software to distinguish between two destinations with the same IP address.                                                                                                                      | <a href="#">Dialing to Destinations with the Same IP Address for MPLS VPNs</a>                                                                         |
|                                                  | MPLS VPN—Carrier Supporting Carrier                                | This feature enables you to set up and create an MPLS VPN CSC network that uses LDP to transport MPLS labels and an IGP to transport routes.                                                                                | <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a>       |
|                                                  | MPLS VPN ID                                                        | This feature enables you to identify MPLS VPNs by a VPN identification number, as described in RFC 2685.                                                                                                                    | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                        |
| 12.2(8)T<br>(cont.)                              | MPLS VPN—OSPF and Sham-Link Support                                | This feature allows you to configure a sham-link that directs traffic between VPN client sites over the MPLS VPN backbone.                                                                                                  | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                     |

**Table 1**      **Supported MPLS VPN Features (continued)**

| <b>Release</b> | <b>Feature Name</b>                    | <b>Feature Description</b>                                                                                                                                                              | <b>Where Documented</b>                                                                                                                                |
|----------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(2)T       | iBGP Multipath Load Sharing            | This feature enables the BGP speaking router to select multiple iBGP paths as the best paths to a destination.                                                                          | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                          |
| 12.1(5)T       | Inter-Autonomous Systems for MPLS VPNs | This feature enables an MPLS VPN to span service providers and autonomous systems. This feature explains how to configure the Inter-AS using the ASBRs to exchange VPNv4 addresses.     | <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a> |
| 12.0(5)T       | MPLS Virtual Private Networks          | This feature allows a set of sites that to be interconnected by means of an MPLS provider core network. At each customer site, one or more CE routers attach to one or more PE routers. | <a href="#">Configuring MPLS Layer 3 VPNs</a>                                                                                                          |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# Configuring MPLS Layer 3 VPNs

---

A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers. This module explains how to create an MPLS VPN.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for MPLS Layer 3 VPNs” section on page 36](#).

## Contents

- [Prerequisites for MPLS Layer 3 VPNs, page 2](#)
- [Restrictions for MPLS Layer 3 VPNs, page 2](#)
- [Information about MPLS Layer 3 VPNs](#)
- [How to Configure MPLS Layer 3 VPNs](#)
- [Configuration Examples for MPLS VPNs, page 29](#)
- [Additional References, page 35](#)
- [Feature Information for MPLS Layer 3 VPNs, page 36](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for MPLS Layer 3 VPNs

Before configuring MPLS Layer 3 VPNs, you should have MPLS, Label Distribution Protocol (LDP), and Cisco Express Forwarding (CEF) installed in your network. All routers in the core, including the PE routers, must be able to support CEF and MPLS forwarding. See [“Assessing the Needs of MPLS VPN Customers” section on page 9](#) for more information.

## Restrictions for MPLS Layer 3 VPNs

When configuring static routes in an MPLS or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.xT, 12.xM, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later. Use the following guidelines when configuring static routes.

### Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in MPLS environment:

```
ip route destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

### Unsupported Static Routes in an MPLS Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

```
ip route destination-prefix mask next-hop1
ip route destination-prefix mask next-hop2
```

Use the *interface* and *next-hop* arguments when specifying static routes.

### Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop and interface are in the same VRF:

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask* **interface1 next-hop1**  
**ip route vrf** *vrf-name destination-prefix mask* **interface2 next-hop2**

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet Gateway.

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*  
(This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

### Unsupported Static Routes in an MPLS VPN Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

```
ip route vrf destination-prefix mask next-hop-address global
```

The following **ip route** commands are not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

```
ip route vrf destination-prefix mask next-hop1 global
ip route vrf destination-prefix mask next-hop2 global
```

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

```
ip route vrf vrf-name destination-prefix mask next-hop1
ip route vrf vrf-name destination-prefix mask next-hop2
```

### Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table on the CE side. For example, the following command is supported when the destination-prefix is the CE router's loopback address, as in EBGp multihop cases.

```
ip route vrf vrf-name destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static non-recursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 nexthop1
ip route destination-prefix mask interface2 nexthop2
```

# Information about MPLS Layer 3 VPNs

Before configuring MPLS Layer 3 VPNs, you should understand the following concepts:

- [MPLS VPN Definition, page 4](#)
- [How an MPLS VPN Works, page 5](#)
- [Major Components of MPLS VPNs, page 7](#)
- [Benefits of an MPLS VPN, page 7](#)

## MPLS VPN Definition

Before defining an MPLS VPN, you need to define a VPN in general. A VPN is:

- An IP-based network delivering private network services over a public infrastructure
- A set of sites that are allowed to communicate with each other privately over the Internet or other public or private networks

Conventional VPNs are created by configuring a full mesh of tunnels or permanent virtual circuits (PVCs) to all sites in a VPN. This type of VPN is not easy to maintain or expand, because adding a new site requires changing each edge device in the VPN.

MPLS-based VPNs are created in Layer 3 and are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without the customer's involvement.

MPLS VPNs are easier to manage and expand than conventional VPNs. When a new site is added to an MPLS VPN, only the service provider's edge router that provides services to the customer site needs to be updated.

The different parts of the MPLS VPN are described as follows:

- **Provider (P) router**—Router in the core of the provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS label in each route assigned by the PE router) to routed packets. VPN labels are used to direct data packets to the correct egress router.
- **PE router**—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.
- **Customer (C) router**—Router in the ISP or enterprise network.
- **Customer edge router**—Edge router on the network of the ISP that connects to the PE router on the network. A CE router must interface with a PE router.

[Figure 1](#) shows a basic MPLS VPN.

**Figure 1**      **Basic MPLS VPN Terminology**



## How an MPLS VPN Works

MPLS VPN functionality is enabled at the edge of an MPLS network. The PE router performs the following:

- Exchanges routing updates with the CE router
- Translates the CE routing information into VPNv4 routes
- Exchanges VPNv4 routes with other PE routers through the Multiprotocol Border Gateway Protocol (MP-BGP)

## How Virtual Routing/Forwarding Tables Work in an MPLS VPN

Each VPN is associated with one or more virtual routing and forwarding (VRF) instances. A VRF defines the VPN membership of a customer site attached to a PE router. A VRF consists of the following components:

- An IP routing table
- A derived CEF table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocol parameters that control the information that is included in the routing table

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A site can be a member of multiple VPNs. However, a site can associate with only one VRF. A site's VRF contains all the routes available to the site from the VPNs of which it is a member.

Packet forwarding information is stored in the IP routing table and the CEF table for each VRF. A separate set of routing and CEF tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN, and also prevent packets that are outside a VPN from being forwarded to a router within the VPN.

## How VPN Routing Information Is Distributed in an MPLS VPN

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. VPN routing information is distributed as follows:

- When a VPN route that is learned from a CE router is injected into BGP, a list of VPN route target extended community attributes is associated with it. Typically the list of route target community extended values is set from an export list of route targets associated with the VRF from which the route was learned.
- An import list of route target extended communities is associated with each VRF. The import list defines route target extended community attributes that a route must have in order for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target extended communities A, B, and C, then any VPN route that carries any of those route target extended communities—A, B, *or* C—is imported into the VRF.

## BGP Distribution of VPN Routing Information

A PE router can learn an IP prefix from the following sources:

- A CE router by static configuration
- A BGP session with the CE router
- A Routing Information Protocol (RIP) exchange with the CE router

The IP prefix is a member of the IPv4 address family. After the PE router learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses. The route distinguisher used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the VRF on the PE router.

BGP distributes reachability information for VPN-IPv4 prefixes for each VPN. BGP communication takes place at two levels:

- Within IP domains, known as an autonomous system (interior BGP [IBGP])
- Between autonomous systems (external BGP [EBGP]).

PE-PE or PE-RR (route reflector) sessions are IBGP sessions, and PE-CE sessions are EBGP sessions.

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions (refer to RFC 2283, *Multiprotocol Extensions for BGP-4*), which define support for address families other than IPv4. Using the extensions ensures that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other.

## MPLS Forwarding

Based on routing information stored in the VRF IP routing table and VRF CEF table, packets are forwarded to their destination using MPLS.

A PE router binds a label to each customer prefix learned from a CE router and includes the label in the network reachability information for the prefix that it advertises to other PE routers. When a PE router forwards a packet received from a CE router across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet,

it pops the label and uses it to direct the packet to the correct CE router. Label forwarding across the provider backbone is based on either dynamic label switching or traffic engineered paths. A customer data packet carries two levels of labels when traversing the backbone:

- The top label directs the packet to the correct PE router.
- The second label indicates how that PE router should forward the packet to the CE router.

## Major Components of MPLS VPNs

An MPLS-based VPN network has three major components:

- **VPN route target communities**—A VPN route target community is a list of all members of a VPN community. VPN route targets need to be configured for each VPN community member.
- **Multiprotocol BGP (MP-BGP) peering of VPN community PE routers**—MP-BGP propagates VRF reachability information to all members of a VPN community. MP-BGP peering needs to be configured in all PE routers within a VPN community.
- **MPLS forwarding**—MPLS transports all traffic between all VPN community members across a VPN service-provider network.

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs. However, a site can associate with only one VRF. A customer-site VRF contains all the routes available to the site from the VPNs of which it is a member.

## Benefits of an MPLS VPN

MPLS VPNs allow service providers to deploy scalable VPNs and build the foundation to deliver value-added services, including:

**Connectionless Service**—A significant technical advantage of MPLS VPNs is that they are connectionless. The Internet owes its success to its basic technology, TCP/IP. TCP/IP is built on packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate. To establish privacy in a connectionless IP environment, current VPN solutions impose a connection-oriented, point-to-point overlay on the network. Even if it runs over a connectionless network, a VPN cannot take advantage of the ease of connectivity and multiple services available in connectionless networks. When you create a connectionless VPN, you do not need tunnels and encryption for network privacy, thus eliminating significant complexity.

**Centralized Service**—Building VPNs in Layer 3 allows delivery of targeted services to a group of users represented by a VPN. A VPN must give service providers more than a mechanism for privately connecting users to intranet services. It must also provide a way to flexibly deliver value-added services to targeted customers. Scalability is critical, because customers want to use services privately in their intranets and extranets. Because MPLS VPNs are seen as private intranets, you may use new IP services such as:

- Multicast
- Quality of service (QoS)
- Telephony support within a VPN
- Centralized services including content and web hosting to a VPN

You can customize several combinations of specialized services for individual customers. For example, a service that combines IP multicast with a low-latency service class enables video conferencing within an intranet.

**Scalability**—If you create a VPN using connection-oriented, point-to-point overlays, Frame Relay, or ATM virtual connections (VCs), the VPN's key deficiency is scalability. Specifically, connection-oriented VPNs without fully meshed connections between customer sites are not optimal. MPLS-based VPNs instead use the peer model and Layer 3 connectionless architecture to leverage a highly scalable VPN solution. The peer model requires a customer site to peer with only one PE router as opposed to all other customer edge (CE) routers that are members of the VPN. The connectionless architecture allows the creation of VPNs in Layer 3, eliminating the need for tunnels or VCs.

Other scalability issues of MPLS VPNs are due to the partitioning of VPN routes between PE routers and the further partitioning of VPN and IGP routes between PE routers and provider (P) routers in a core network.

- PE routers must maintain VPN routes for those VPNs who are members.
- P routers do not maintain any VPN routes.

This increases the scalability of the provider's core and ensures that no one device is a scalability bottleneck.

**Security**—MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN.

Security is provided in the following areas:

- At the edge of a provider network, ensuring packets received from a customer are placed on the correct VPN.
- At the backbone, VPN traffic is kept separate. Malicious spoofing (an attempt to gain access to a PE router) is nearly impossible because the packets received from customers are IP packets. These IP packets must be received on a particular interface or subinterface to be uniquely identified with a VPN label.

**Easy to Create**—To take full advantage of VPNs, customers must be able to easily create new VPNs and user communities. Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required. You can add sites to intranets and extranets and form closed user groups. Managing VPNs in this manner enables membership of any given site in multiple VPNs, maximizing flexibility in building intranets and extranets.

**Flexible Addressing**—To make a VPN service more accessible, customers of a service provider can design their own addressing plan, independent of addressing plans for other service provider customers. Many customers use private address spaces, as defined in RFC 1918, and do not want to invest the time and expense of converting to public IP addresses to enable intranet connectivity. MPLS VPNs allow customers to continue to use their present address spaces without network address translation (NAT) by providing a public and private view of the address. A NAT is required only if two VPNs with overlapping address spaces want to communicate. This enables customers to use their own unregistered private addresses, and communicate freely across a public IP network.

**Integrated Quality of Service (QoS) Support**—QoS is an important requirement for many IP VPN customers. It provides the ability to address two fundamental VPN requirements:

- Predictable performance and policy implementation
- Support for multiple levels of service in an MPLS VPN

Network traffic is classified and labeled at the edge of the network before traffic is aggregated according to policies defined by subscribers and implemented by the provider and transported across the provider core. Traffic at the edge and core of the network can then be differentiated into different classes by drop probability or delay.

**Straightforward Migration**—For service providers to quickly deploy VPN services, use a straightforward migration path. MPLS VPNs are unique because you can build them over multiple network architectures, including IP, ATM, Frame Relay, and hybrid networks.

Migration for the end customer is simplified because there is no requirement to support MPLS on the CE router and no modifications are required to a customer's intranet.

## How to Configure MPLS Layer 3 VPNs

To configure and verify VPNs, perform the tasks described in the following sections:

- [Configuring the Core Network, page 9](#) (required)
- [Connecting the MPLS VPN Customers, page 13](#) (required)
- [Verifying Connectivity Between MPLS VPN Sites, page 27](#) (optional)

### Configuring the Core Network

Configuring the core network includes the following tasks:

- [Assessing the Needs of MPLS VPN Customers, page 9](#) (required)
- [Configuring Routing Protocols in the Core, page 10](#) (required)
- [Configuring MPLS in the Core, page 10](#) (required)
- [Determining if CEF Is Enabled in the Core, page 10](#) (required)
- [Configuring Multiprotocol BGP on the PE Routers and Route Reflectors, page 11](#) (required)

### Assessing the Needs of MPLS VPN Customers

Before you configure an MPLS VPN, you need to identify the core network topology so that it can best serve MPLS VPN customers. Perform this task to identify the core network topology.

#### SUMMARY STEPS

1. Identify the size of the network.
2. Identify the routing protocols.
3. Determine if you need MPLS High Availability support.
4. Determine if you need BGP load sharing and redundant paths.

## DETAILED STEPS

|        | Command or Action                                                                | Purpose                                                                                                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Identify the size of the network.                                                | Identify the following to determine the number of routers and ports you need: <ul style="list-style-type: none"> <li>• How many customers do you need to support?</li> <li>• How many VPNs are needed per customer?</li> <li>• How many virtual routing and forwarding instances are there for each VPN?</li> </ul> |
| Step 2 | Identify the routing protocols in the core.                                      | Determine which routing protocols you need in the core network.                                                                                                                                                                                                                                                     |
| Step 3 | Determine if you need MPLS VPN High Availability support.                        | MPLS VPN Nonstop Forwarding and Graceful Restart are supported on select routers and Cisco IOS releases. Contact Cisco Support for the exact requirements and hardware support.                                                                                                                                     |
| Step 4 | Determine if you need BGP load sharing and redundant paths in the MPLS VPN core. | See <a href="#">Load Sharing MPLS VPN Traffic</a> for configuration steps.                                                                                                                                                                                                                                          |

## Configuring Routing Protocols in the Core

To configure a routing protocol—BGP, OSPF, IS-IS, EIGRP, static—see [Configuring IP Routing Protocols](#).

## Configuring MPLS in the Core

To enable MPLS on all routers in the core, you must configure a label distribution protocol. You can use either of the following as a label distribution protocol:

- MPLS Label Distribution Protocol (LDP). For configuration information, see the [Configuring MPLS Label Distribution Protocol \(LDP\)](#).
- MPLS Traffic Engineering Resource Reservation Protocol (RSVP). For configuration information, see [Configuring MPLS Traffic Engineering](#).

## Determining if CEF Is Enabled in the Core

Cisco Express Forwarding (CEF) must be enabled all routers in the core, including the PE routers. For information about how to determine if CEF is enabled, see [Configuring Basic Cisco Express Forwarding—Improving Performance, Scalability, and Resiliency in Dynamic Network](#).

## Configuring Multiprotocol BGP on the PE Routers and Route Reflectors

Perform this task to configure multiprotocol BGP (MP-BGP) connectivity on the PE routers and route reflectors.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **address-family vpv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

### DETAILED STEPS

|        | Command or Action                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                  | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                     | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>no bgp default ipv4-unicast</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default ipv4-unicast | (Optional) Disables the IPv4 unicast address family on all neighbors. <ul style="list-style-type: none"> <li>• Use the <b>no</b> form of the <b>bgp default ipv4-unicast</b> command if you are using this neighbor for MPLS routes only.</li> </ul>                                                                                                                                                                                       |

|         | Command or Action                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <pre>neighbor {ip-address   peer-group-name} remote-as as-number</pre> <p><b>Example:</b><br/>Router(config-router)# neighbor pp.0.0.1<br/>remote-as 100</p>                  | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 6  | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router)# neighbor pp.0.0.1<br/>activate</p>                                  | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 7  | <pre>address-family vpnv4 [unicast]</pre> <p><b>Example:</b><br/>Router(config-router)# address-family vpnv4</p>                                                              | <p>Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.</p> <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                   |
| Step 8  | <pre>neighbor {ip-address   peer-group-name} send-community extended</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1<br/>send-community extended</p> | <p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                               |
| Step 9  | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1<br/>activate</p>                               | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 10 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                                       | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                           |

## Troubleshooting Tips

You can enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. If this command is not successful, enter a **debug ip bgp x.x.x.x events** command, where *x.x.x.x* is the IP address of the neighbor.

## Connecting the MPLS VPN Customers

To connect the MPLS VPN customers to the VPN, perform the following tasks:

- [Defining VRFs on the PE Routers to Enable Customer Connectivity, page 13](#) (required)
- [Configuring VRF Interfaces on PE Routers for Each VPN Customer, page 14](#) (required)
- [Configuring Routing Protocols Between the PE and CE Routers, page 15](#) (required)

### Defining VRFs on the PE Routers to Enable Customer Connectivity

To define VPN routing and forwarding (VRF) instances, perform this task.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map** *route-map*
7. **exit**

#### DETAILED STEPS

|        | Command or Action                                                                   | Purpose                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                              | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal      | Enters global configuration mode.                                                                                                                                |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# ip vrf vpn1 | Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode.<br><br>• The <i>vrf-name</i> argument is the name assigned to a VRF. |

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <pre>rd route-distinguisher</pre> <p><b>Example:</b><br/>Router(config-vrf)# rd 100:1</p>                                                            | <p>Creates routing and forwarding tables.</p> <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats: <ul style="list-style-type: none"> <li>16-bit AS number: your 32-bit number, for example, 101:3</li> <li>32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul>                                                                                                                                                                                                                    |
| Step 5 | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf)# route-target import 100:1</p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |
| Step 6 | <pre>import map route-map</pre> <p><b>Example:</b><br/>Router(config-vrf)# import map vpn1-route-map</p>                                             | <p>(Optional) Configures an import route map for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-vrf)# exit</p>                                                                                  | <p>(Optional) Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Configuring VRF Interfaces on PE Routers for Each VPN Customer

To associate a VRF with an interface or subinterface on the PE routers, perform this task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                               | Enters global configuration mode.                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 5/0         | Specifies the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul> |
| Step 4 | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1 | Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                            |
| Step 5 | <b>end</b><br><br>Router(config-if)# end                                                                     | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                               |

## Configuring Routing Protocols Between the PE and CE Routers

Configure the PE router with the same routing protocol that the CE router uses. You can configure the following routing protocols:

- [Configuring BGP as the Routing Protocol Between the PE and CE Routers, page 15](#)
- [Configuring RIPv2 as the Routing Protocol Between the PE and CE Routers, page 17](#)
- [Configuring Static Routes Between the PE and CE Routers, page 19](#)
- [Configuring OSPF as the Routing Protocol Between the PE and CE Routers, page 21](#)
- [Configuring EIGRP as the Routing Protocol Between the PE and CE Routers, page 23](#)
- [Configuring EIGRP Redistribution in the MPLS VPN, page 25](#)

## Configuring BGP as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions using BGP, perform this task.

## SUMMARY STEPS

- enable**
- configure terminal**
- router bgp** *as-number*

4. **address-family ipv4** [**multicast** | **unicast** | **vrf vrf-name**]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as as-number**
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **exit-address-family**
8. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                          | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                     | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <p><b>router bgp</b> <i>as-number</i></p> <p><b>Example:</b><br/>Router(config)# router bgp 100</p>                                                                        | <p>Configures a BGP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                        |
| Step 4 | <p><b>address-family ipv4</b> [<b>multicast</b>   <b>unicast</b>   <b>vrf vrf-name</b>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf vpn1</p> | <p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>• The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>• The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>• The <b>vrf vrf-name</b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |

|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>remote-as</b> <i>as-number</i></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1 remote-as 200</p> | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 6 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1 activate</p>                        | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 7 | <p><b>exit-address-family</b></p> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                                                 | <p>Exits address family configuration mode.</p>                                                                                                                                                                                                                                                                                                                                            |
| Step 8 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-router)# end</p>                                                                                                                    | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                           |

### Configuring RIPv2 as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions using RIPv2, perform this task.

#### SUMMARY STEPS

- enable**
- configure terminal**
- router rip**
- version** {1 | 2}
- address-family** ipv4 [multicast | unicast | vrf *vrf-name*]
- network** *ip-address*
- redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
- exit-address-family**
- end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <code>router rip</code><br><br><b>Example:</b><br>Router(config)# router rip                                                                                                                                                                                                                                   | Enables RIP.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <code>version {1   2}</code><br><br><b>Example:</b><br>Router(config-router)# version 2                                                                                                                                                                                                                        | Specifies a Routing Information Protocol (RIP) version used globally by the router.                                                                                                                                                                                                                                                                                                                                                                           |
| Step 5 | <code>address-family ipv4 [multicast   unicast   vrf vrf-name]</code><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn1                                                                                                                                                            | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 6 | <code>network ip-address</code><br><br><b>Example:</b><br>Router(config-router-af)# network 192.168.7.0                                                                                                                                                                                                        | Enables RIP on the PE-to-CE link.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 7 | <code>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</code><br><br><b>Example:</b><br>Router(config-router-af)# redistribute bgp 200 | Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>For the RIPv2 routing protocol, use the <b>redistribute bgp as-number</b> command.</li> </ul> See the <a href="#">redistribute</a> command for information about other arguments and keywords.                                                                                                                                               |

|        | Command or Action                                                                                  | Purpose                                   |
|--------|----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 8 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family | Exits address family configuration mode.  |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                    | (Optional) Exits to privileged EXEC mode. |

## Configuring Static Routes Between the PE and CE Routers

To configure PE-to-CE routing sessions that use static routes, perform this task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route vrf *vrf-name***
4. **address-family ipv4 [multicast | unicast | vrf *vrf-name*]**
5. **redistribute *protocol* [*process-id*] { **level-1** | **level-1-2** | **level-2** } [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** { **internal** | **external 1** | **external 2** }] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]**
6. **redistribute *protocol* [*process-id*] { **level-1** | **level-1-2** | **level-2** } [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** { **internal** | **external 1** | **external 2** }] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]**
7. **exit-address-family**
8. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                  | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                                                                                                                             | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <p><b>ip route vrf vrf-name</b></p> <p><b>Example:</b><br/>Router(config)# ip route vrf 200</p>                                                                                                                                                                                                                    | <p>Defines static route parameters for every PE-to-CE session.</p>                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 4 | <p><b>address-family ipv4 [multicast   unicast   vrf vrf-name]</b></p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf vpn1</p>                                                                                                                                                              | <p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <p><b>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</b></p> <p><b>Example:</b><br/>Router(config-router-af)# redistribute static</p>    | <p>Redistributes routes from one routing domain into another routing domain.</p> <ul style="list-style-type: none"> <li>To redistribute VRF static routes into the VRF BGP table, use the <b>redistribute static</b> command.</li> </ul> <p>See the <a href="#">redistribute</a> command for information about other arguments and keywords.</p>                                                                                                                     |
| Step 6 | <p><b>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</b></p> <p><b>Example:</b><br/>Router(config-router-af)# redistribute connected</p> | <p>Redistributes routes from one routing domain into another routing domain.</p> <ul style="list-style-type: none"> <li>To redistribute directly connected networks into the VRF BGP table, use the <b>redistribute connected</b> command.</li> </ul> <p>See the <a href="#">redistribute</a> command for information about other arguments and keywords.</p>                                                                                                        |

|        | Command or Action                                                                                  | Purpose                                   |
|--------|----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 7 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family | Exits address family configuration mode.  |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                    | (Optional) Exits to privileged EXEC mode. |

### Configuring OSPF as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions that use OSPF, perform this task.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **network** *ip-address wildcard-mask area* *area-id*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
7. **exit-address-family**
8. **end**

#### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|        | Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>router ospf process-id [vrf vpn-name]</pre> <p><b>Example:</b><br/>Router(config)# router ospf 1 vrf grc</p>                                                                                                                                                                                                          | <p>Enables OSPF routing and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>process-id</i> argument identifies the OSPF process.</li> <li>The <b>vrf</b> keyword and <i>vpn-name</i> argument identify a VPN. Create a separate OSPF process for each VRF that will receive VPN routes.</li> </ul>                                                                                                                                                                                                                                                                                    |
| Step 4 | <pre>network ip-address wildcard-mask area area-id</pre> <p><b>Example:</b><br/>Router(config-router)# network 192.168.129.16 0.0.0.3 area 20</p>                                                                                                                                                                          | <p>Defines the interfaces on which OSPF runs and to defines the area ID for those interfaces.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument identifies the IP address.</li> <li>The <i>wildcard-mask</i> argument identifies the IP-address-type mask that includes “don't care” bits.</li> <li>The <i>area-id</i> argument identifies the area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. To associate areas with IP subnets, specify a subnet address as the value of the <i>area-id</i> argument.</li> </ul> |
| Step 5 | <pre>address-family ipv4 [multicast   unicast   vrf vrf-name]</pre> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf vpn1</p>                                                                                                                                                                         | <p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>                                                                                                                                                        |
| Step 6 | <pre>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</pre> <p><b>Example:</b><br/>Router(config-router-af)# redistribute rip metric 1 subnets</p> | <p>Redistributes routes from one routing domain into another routing domain.</p> <p>You may need to include several protocols to ensure that all IBGP routes are distributed into the VRF.</p> <p>See the <a href="#">redistribute</a> command for information about other arguments and keywords.</p>                                                                                                                                                                                                                                                                                                                    |

|        | Command or Action                                                                                  | Purpose                                   |
|--------|----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 7 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family | Exits address family configuration mode.  |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                    | (Optional) Exits to privileged EXEC mode. |

### Configuring EIGRP as the Routing Protocol Between the PE and CE Routers

Using Enhanced Interior Gateway Routing Protocol (EIGRP) between the PE and CE routers allows you to transparently connect EIGRP customer networks through an MPLS-enabled BGP core network so that EIGRP routes are redistributed through the VPN across the BGP network as internal BGP (iBGP) routes.

To configure PE-to-CE routing sessions that use EIGRP, perform this task.

#### Prerequisites

BGP must be configured in the network core.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `router bgp as-number`
4. `no synchronization`
5. `neighbor ip-address remote-as as-number`
6. `neighbor ip-address update-source loopback interface-number`
7. `address-family vpnv4`
8. `neighbor ip-address activate`
9. `neighbor ip-address send-community extended`
10. `exit-address-family`
11. `address-family ipv4 vrf vrf-name`
12. `redistribute eigrp as-number s [metric metric-value][route-map map-name]`
13. `no synchronization`
14. `exit-address-family`
15. `end`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                       |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 10                                                                               | Enters router configuration mode, and creates a BGP routing process.                                                                                                                                                                                                    |
| Step 4 | <b>no synchronization</b><br><br><b>Example:</b><br>Router(config-router)# no synchronization                                                                     | Configures BGP to send advertisements without waiting to synchronize with the IGP.                                                                                                                                                                                      |
| Step 5 | <b>neighbor ip-address remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>remote-as 10                                 | Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>In this step, you are establishing an iBGP session with the PE router that is connected to the CE router at the other CE site.</li> </ul>                         |
| Step 6 | <b>neighbor ip-address update-source loopback interface-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>update-source loopback 0 | Configures BGP to use any operational interface for TCP connections. <ul style="list-style-type: none"> <li>This configuration step is not required. However, the BGP routing process will be less susceptible to the affects of interface or link flapping.</li> </ul> |
| Step 7 | <b>address-family vpnv4</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                                 | Enters address family configuration mode for configuring routing sessions that use standard IPv4 address prefixes, such as BGP, RIP, and static routing sessions.                                                                                                       |
| Step 8 | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>activate                                             | Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>In this step, you are activating the exchange of VPNv4 routing information between the PE routers.</li> </ul>                                                     |
| Step 9 | <b>neighbor ip-address send-community extended</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>send-community extended               | Configures the local router to send extended community attribute information to the specified neighbor. <ul style="list-style-type: none"> <li>This step is required for the exchange of EIGRP extended community attributes.</li> </ul>                                |

|         | Command or Action                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                      |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <code>exit-address-family</code><br><br><b>Example:</b><br><code>Router(config-router-af)# exit-address-family</code>                                                       | Exits address family configuration mode and enters router configuration mode.                                                                                                                                                                                |
| Step 11 | <code>address-family ipv4 vrf vrf-name</code><br><br><b>Example:</b><br><code>Router(config-router)# address-family ipv4 vrf RED</code>                                     | Configures an IPv4 address-family for the EIGRP VRF and enters address family configuration mode. <ul style="list-style-type: none"> <li>An address-family VRF needs to be configured for each EIGRP VRF that runs between the PE and CE routers.</li> </ul> |
| Step 12 | <code>redistribute eigrp as-number [metric metric-value][route-map map-name]</code><br><br><b>Example:</b><br><code>Router(config-router-af)# redistribute eigrp 101</code> | Redistributes the EIGRP VRF into BGP. <ul style="list-style-type: none"> <li>The autonomous system number from the CE network is configured in this step.</li> </ul>                                                                                         |
| Step 13 | <code>no synchronization</code><br><br><b>Example:</b><br><code>Router(config-router-af)# no synchronization</code>                                                         | Configures BGP to send advertisements without waiting to synchronize with the IGP.                                                                                                                                                                           |
| Step 14 | <code>exit-address-family</code><br><br><b>Example:</b><br><code>Router(config-router-af)# exit-address-family</code>                                                       | Exits address family configuration mode and enters router configuration mode.                                                                                                                                                                                |
| Step 15 | <code>end</code><br><br><b>Example:</b><br><code>Router(config-router)# end</code>                                                                                          | Exits router configuration mode and enters privileged EXEC mode.                                                                                                                                                                                             |

### Configuring EIGRP Redistribution in the MPLS VPN

Perform this task to every PE router that provides VPN services to enable EIGRP redistribution in the MPLS VPN.

#### Prerequisites

The metric must be configured for routes from external EIGRP autonomous systems and non-EIGRP networks before these routes can be redistributed into an EIGRP CE router. The metric can be configured in the redistribute statement using the **redistribute (IP)** command or configured with the **default-metric (EIGRP)** command. If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route will not be advertised to the CE router.

#### Restrictions

Redistribution between native EIGRP VRFs is not supported. This is designed behavior.

#### SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **router eigrp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **network** *ip-address wildcard-mask*
6. **redistribute bgp** {*as-number*} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map-name*]
7. **autonomous-system** *as-number*
8. **exit-address-family**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>router eigrp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router eigrp 1                                                                                                                                                       | Enters router configuration mode and creates an EIGRP routing process. <ul style="list-style-type: none"> <li>The EIGRP routing process for the PE router is created in this step.</li> </ul>                                                                                                                                                                                  |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                                                          | Enters address-family configuration mode and creates a VRF. <ul style="list-style-type: none"> <li>The VRF name must match the VRF name that was created in the previous section.</li> </ul>                                                                                                                                                                                   |
| Step 5 | <b>network</b> <i>ip-address wildcard-mask</i><br><br><b>Example:</b><br>Router(config-router-af)# network 172.16.0.0 0.0.255.255                                                                                                                   | Specifies the network for the VRF. <ul style="list-style-type: none"> <li>The network statement is used to identify which interfaces to include in EIGRP. The VRF must be configured with addresses that fall within the wildcard-mask range of the network statement.</li> </ul>                                                                                              |
| Step 6 | <b>redistribute bgp</b> { <i>as-number</i> } [ <b>metric</b> <i>bandwidth delay reliability load mtu</i> ] [ <b>route-map</b> <i>map-name</i> ]<br><br><b>Example:</b><br>Router(config-router-af)# redistribute bgp 10 metric 10000 100 255 1 1500 | Redistributes BGP into the EIGRP. <ul style="list-style-type: none"> <li>The autonomous system number and metric of the BGP network is configured in this step. BGP must be redistributed into EIGRP for the CE site to accept the BGP routes that carry the EIGRP information. A metric must also be specified for the BGP network and is configured in this step.</li> </ul> |

|        | Command or Action                                                                                                               | Purpose                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Step 7 | <code>autonomous-system as-number</code><br><br><b>Example:</b><br><code>Router(config-router-af)# autonomous-system 101</code> | Specifies the autonomous system number of the EIGRP network for the customer site. |
| Step 8 | <code>exit-address-family</code><br><br><b>Example:</b><br><code>Router(config-router-af)# exit-address-family</code>           | Exits address family configuration mode and enters router configuration mode.      |
| Step 9 | <code>end</code><br><br><b>Example:</b><br><code>Router(config-router)# end</code>                                              | Exits router configuration mode and enters privileged EXEC mode.                   |

## Verifying the VPN Configuration

A route distinguisher must be configured for the VRF, and MPLS must be configured on the interfaces that carry the VRF. Use the **show ip vrf** command to verify the route distinguisher (RD) and interface that are configured for the VRF.

### SUMMARY STEPS

1. **show ip vrf**

### DETAILED STEPS

---

#### Step 1 **show ip vrf**

Use this command to display the set of defined VRF instances and associated interfaces. The output also maps the VRF instances to the configured route distinguisher.

---

## Verifying Connectivity Between MPLS VPN Sites

To verify that the local and remote CE routers can communicate across the MPLS core, perform the following tasks:

- [Verifying IP Connectivity from CE Router to CE Router Across the MPLS Core, page 27](#)
- [Verifying that the Local and Remote CE Routers are in the Routing Table, page 28](#)

## Verifying IP Connectivity from CE Router to CE Router Across the MPLS Core

Perform this task to verify IP connectivity from CE router to CE router across the MPLS VPN.

### SUMMARY STEPS

1. **enable**

2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]
5. **disable**

## DETAILED STEPS

---

### Step 1 **enable**

Use this command to enable privileged EXEC mode.

### Step 2 **ping** [*protocol*] {*host-name* | *system-address*}

Use this command to diagnose basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks. Use the **ping** command to verify the connectivity from one CE router to another.

### Step 3 **trace** [*protocol*] [*destination*]

Use this command to discover the routes that packets take when traveling to their destination. Use the **trace** command to verify the path that a packet goes through before reaching the final destination. The **trace** command can help isolate a trouble spot if two routers cannot communicate.

### Step 4 **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]

Use this command to display the current state of the routing table. Use the *ip-address* argument to verify that CE1 has a route to CE2. Verify the routes learned by CE1. Make sure that the route for CE2 is listed.

---

## Verifying that the Local and Remote CE Routers are in the Routing Table

Perform this task to check that the local and remote CE routers are in the routing table of the PE routers.

## SUMMARY STEPS

1. **enable**
2. **show ip route vrf** *vrf-name* [*prefix*]
3. **show ip cef vrf** *vrf-name* [*ip-prefix*]
4. **exit**

---

### Step 1 **enable**

Use this command to enable privileged EXEC mode.

### Step 2 **show ip route vrf** *vrf-name* [*prefix*]

Use this command to display the IP routing table associated with a VRF. Check that the loopback addresses of the local and remote CE routers are in the routing table of the PE routers.

### Step 3 **show ip cef vrf** *vrf-name* [*ip-prefix*]

Use this command to display the CEF forwarding table associated with a VRF. Check that the prefix of the remote CE router is in the CEF table.

**Step 4**    **exit**

---

## Configuration Examples for MPLS VPNs

- [Configuring an MPLS VPN Using BGP: Example, page 30](#)
- [Configuring an MPLS VPN Using RIP: Example, page 31](#)
- [Configuring an MPLS VPN Using Static Routes: Example, page 32](#)
- [Configuring an MPLS VPN Using OSPF: Example, page 33](#)
- [Configuring an MPLS VPN Using EIGRP: Example, page 34](#)

## Configuring an MPLS VPN Using BGP: Example

This example shows an MPLS VPN that is configured using BGP.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | CE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router ospf 100   network 10.0.0. 0.0.0.0 area 100   network 30.0.0.0 0.255.255.255 area 100 ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   neighbor 34.0.0.1 remote-as 200   neighbor 34.0.0.1 activate   neighbor 34.0.0.1 as-override   neighbor 34.0.0.1 advertisement-interval 5   no auto-summary   no synchronization   exit-address-family </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router bgp 200   bgp log-neighbor-changes   neighbor 34.0.0.2 remote-as 100 ! address-family ipv4   redistribute connected   neighbor 34.0.0.2 activate   neighbor 34.0.0.2 advertisement-interval 5   no auto-summary   no synchronization   exit-address-family </pre> |

## Configuring an MPLS VPN Using RIP: Example

This example shows an MPLS VPN that is configured using RIP.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | CE Configuration                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router rip   version 2   timers basic 30 60 60 120 ! address-family ipv4 vrf vpn1   version 2   redistribute bgp 100 metric transparent   network 34.0.0.0   distribute-list 20 in   no auto-summary   exit-address-family ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute rip   no auto-summary   no synchronization   exit-address-family           </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable  router rip   version 2   timers basic 30 60 60 120   redistribute connected   network 10.0.0.0   network 34.0.0.0   no auto-summary           </pre> |

## Configuring an MPLS VPN Using Static Routes: Example

This example shows an MPLS VPN that is configured using static routes.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CE Configuration                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router ospf 100 network 10.0.0. 0.0.0.0 area 100 network 30.0.0.0 0.255.255.255 area 100 ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute static   no auto-summary   no synchronization   exit-address-family ! ip route vrf vpn1 10.0.0.9 255.255.255.255 34.0.0.1 ip route vrf vpn1 34.0.0.0 255.0.0.0 34.0.0.1 </pre> | <pre> ip cef ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! ip route 10.0.0.9 255.255.255.255 34.0.0.2 3 ip route 31.0.0.0 255.0.0.0 34.0.0.2 3 </pre> |

## Configuring an MPLS VPN Using OSPF: Example

This example shows an MPLS VPN that is configured using OSPF.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | CE Configuration                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! router ospf 1000 vrf vpn1   log-adjacency-changes   redistribute bgp 100 metric-type 1 subnets   network 10.0.0.13 0.0.0.0 area 10000   network 34.0.0.0 0.255.255.255 area 10000 ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute ospf 1000 match internal   external 1 external 2   no auto-summary   no synchronization   exit-address-family </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router ospf 1000   log-adjacency-changes   auto-cost reference-bandwidth 1000   redistribute connected subnets   network 34.0.0.0 0.255.255.255 area 1000   network 10.0.0.0 0.0.0.0 area 1000 </pre> |

## Configuring an MPLS VPN Using EIGRP: Example

This example shows an MPLS VPN that is configured using EIGRP.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | CE Configuration                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip router eigrp 1000   auto-summary ! address-family ipv4 vrf vpn1   redistribute bgp 100 metric 10000 100 255   1 1500   network 34.0.0.0   distribute-list 20 in   no auto-summary   autonomous-system 1000   exit-address-family ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute eigrp   no auto-summary   no synchronization   exit-address-family </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router eigrp 1000   network 34.0.0.0   auto-summary </pre> |

# Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic | Document Title                           |
|---------------|------------------------------------------|
| MPLS          | <a href="#">MPLS Product Information</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for MPLS Layer 3 VPNs

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Layer 3 VPNs

| Feature Name                                                       | Releases                                                                                | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Virtual Private Networks                                      | 12.0(5)T<br>12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.2(14)S<br>12.0(26)S | This feature allows a set of sites that to be interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">MPLS VPN Definition, page 4</a></li> <li>• <a href="#">How an MPLS VPN Works, page 5</a></li> <li>• <a href="#">Major Components of MPLS VPNs, page 7</a></li> <li>• <a href="#">Benefits of an MPLS VPN, page 7</a></li> <li>• <a href="#">How to Configure MPLS Layer 3 VPNs, page 9</a></li> </ul> |
| MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge | 12.0(22)S<br>12.2(15)T<br>12.2(18)S<br>12.0(27)S                                        | This feature allows you to connect customers running EIGRP to an MPLS VPN.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Configuring EIGRP as the Routing Protocol Between the PE and CE Routers, page 23</a></li> <li>• <a href="#">Configuring EIGRP Redistribution in the MPLS VPN, page 25</a></li> </ul>                                                                                                                                                                                                                                                               |
| MPLS Virtual Private Networks (VPN)                                | Cisco IOS XE Release 2.1                                                                | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Table 1**      *Feature Information for MPLS Layer 3 VPNs*

| Feature Name                                                                 | Releases                 | Feature Configuration Information                             |
|------------------------------------------------------------------------------|--------------------------|---------------------------------------------------------------|
| MPLS VPN - OSPF PE-CE Support                                                | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |
| MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |



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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

---

The MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses feature allows an MPLS VPN to span service providers and autonomous systems. This module explains how to enable Autonomous System Boundary Routers (ASBRs) to use Exterior Border Gateway Protocol (EBGP) to exchange IPv4 Network Layer Reachability Information (NLRI) in the form of VPN-IPv4 addresses.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses”](#) section on page 33.

## Contents

- [Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 2](#)
- [Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 3](#)
- [Information About MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 3](#)
- [How to Configure MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 11](#)
- [Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 16](#)
- [Additional References, page 32](#)
- [Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 33](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

- Before you configure EBGp routing between autonomous systems or subautonomous systems in an MPLS VPN, ensure that you have properly configured all MPLS VPN routing instances and sessions. The configuration tasks outlined in this section build from those configuration tasks. Perform the following tasks as described in *Configuring MPLS Layer 3 VPNs*:
  - Define VPN routing instances
  - Configure BGP routing sessions in the MPLS core
  - Configure PE-to-PE routing sessions MPLS core
  - Configure BGP PE-to-CE routing sessions
  - Configure a VPN-IPv4 EBGp session between directly connected ASBRs
- This feature is supported on the Cisco 12000 series router line cards listed in [Table 1](#).

**Table 1 Cisco 12000 Series Line Card Support Added for Cisco IOS Releases**

| Type                             | Line Cards            | Cisco IOS Release Added |
|----------------------------------|-----------------------|-------------------------|
| Packet Over SONET (POS)          | 4-Port OC-3 POS       | 12.0(16)ST              |
|                                  | 1-Port OC-12 POS      |                         |
|                                  | 8-Port OC-3 POS       | 12.0(17)ST              |
|                                  | 16-Port OC-3 POS      |                         |
|                                  | 4-Port OC-12 POS      |                         |
|                                  | 1-Port OC-48 POS      |                         |
|                                  | 4-Port OC-3 POS ISE   | 12.0(22)S               |
|                                  | 8-Port OC-3 POS ISE   |                         |
|                                  | 16 x OC-3 POS ISE     |                         |
|                                  | 4-Port OC-12 POS ISE  |                         |
| 1-Port OC-48 POS ISE             |                       |                         |
| Electrical Interface             | 6-Port DS3            | 12.0(21)ST              |
|                                  | 12-Port DS3           |                         |
|                                  | 6-Port E3             | 12.0(22)S               |
|                                  | 12-Port E3            |                         |
| Ethernet                         | 3-Port GbE            | 12.0(23)S               |
|                                  | 1-Port 10-GbE         | 12.0(24)S               |
|                                  | Modular GbE/FE        |                         |
| Asynchronous Transfer Mode (ATM) | 4-Port OC-3 ATM       | 12.0(16)ST              |
|                                  | 1-Port OC-12 ATM      |                         |
|                                  | 4-Port OC-12 ATM      | 12.0(17)ST              |
|                                  | 8-Port OC-3 ATM       | 12.0(23)S               |
| Channelized Interface            | 2-Port CHOC-3         | 12.0(22)S               |
|                                  | 6-Port Ch T3 (DS1)    |                         |
|                                  | 1-Port CHOC-12 (DS3)  |                         |
|                                  | 1-Port CHOC-12 (OC-3) |                         |
|                                  | 4-Port CHOC-12 ISE    |                         |
|                                  | 1-Port CHOC-48 ISE    |                         |

# Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Multihop VPN-IPv4 EBGp is not supported.

## Information About MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Before configuring this feature, you should understand the following concepts:

- [MPLS VPN Inter-AS Introduction, page 3](#)
- [Benefits of MPLS VPN Inter-AS, page 3](#)
- [Information about Using Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 4](#)
- [How Information is Exchanged in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 4](#)

## MPLS VPN Inter-AS Introduction

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.

## Benefits of MPLS VPN Inter-AS

An MPLS VPN Inter-AS provides the following benefits:

- Allows a VPN to cross more than one service provider backbone

Service providers, running separate autonomous systems, can 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 VPN could only traverse a single BGP autonomous system service provider backbone. This feature allows multiple autonomous systems to form a continuous (and seamless) network between customer sites of a service provider.

- Allows a VPN to exist in different areas

A service provider can 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

Internal Border Gateway Protocol (IBGP) meshing in an autonomous system is 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 NLRI between the subautonomous systems that form the confederation.

## Information about Using Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Separate autonomous systems from different service providers can communicate by exchanging IPv4 NLRI in the form of VPN-IPv4 addresses. The ASBRs use EBGP to exchange that information. Then an Interior Gateway Protocol (IGP) 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 IGP.
- Between autonomous systems, routing information is shared using an EBGP. An EBGP allows a service provider to set up an interdomain routing system that guarantees the loop-free exchange of routing information between separate autonomous systems.

The primary function of an EBGP is to exchange network reachability information between autonomous systems, including information about the list of autonomous system routes. The autonomous systems use EGBP border edge routers to distribute the routes, which include label switching information. Each border edge router rewrites the next-hop and MPLS labels. See the “[How Information is Exchanged in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses](#)” section for more information.

Interautonomous 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 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.

## How Information is Exchanged in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

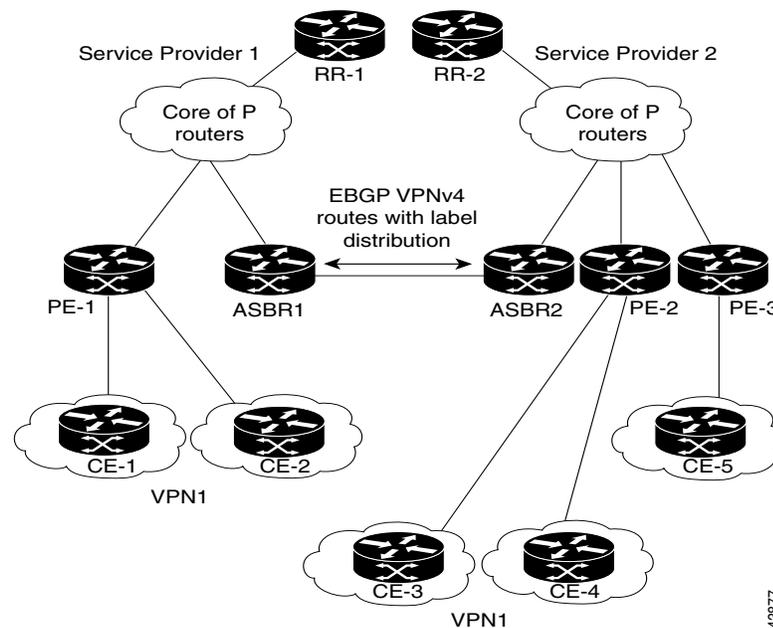
This section contains the following topics:

- [Transmitting Information in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 5](#)
- [Exchanging VPN Routing Information in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 6](#)
- [Packet Forwarding Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses, page 8](#)
- [Using a Confederation for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 9](#)

## Transmitting Information in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Figure 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, ASBR2).

**Figure 1** *EBGP Connection Between Two MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses*



This configuration uses the following process to transmit information:

- Step 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 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.
- Step 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.
- Step 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 address ensures the following:
  - That the next-hop router is always reachable in the service provider (P) backbone network.
  - That 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.)
- Step 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.

- 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 in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

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 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. It makes 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 NLRIs to the IBGP neighbors. Therefore, the ASBRs must allocate a new label when they forward the NLRI to the IBGP neighbors.

**Figure 2** *Exchanging Routes and Labels Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses*

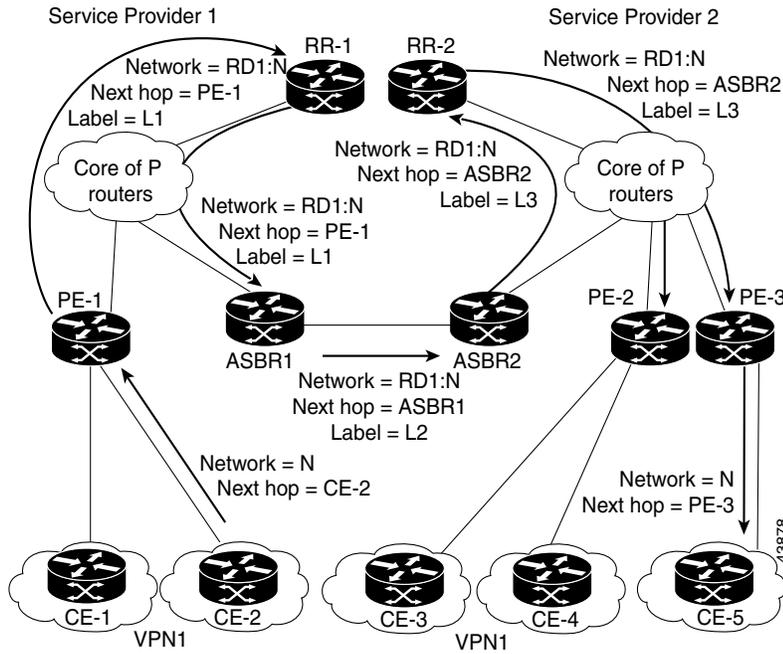
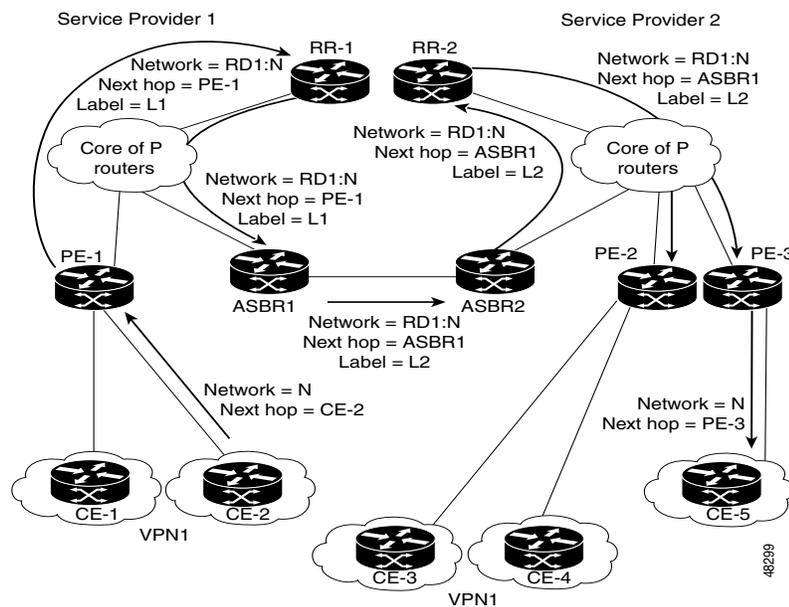


Figure 3 illustrates the exchange of VPN route and label information between autonomous systems. The only difference is that ASBR2 is configured with the **redistribute connected** command, which propagates the host routes to all PEs. The **redistribute connected** command is necessary because ASBR2 is not configured to change the next-hop address.

**Figure 3** *Exchanging Routes and Labels with the redistributed connected Command in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses*



## Packet Forwarding Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses

Figure 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 by means of 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 multilevel 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 4 Forwarding Packets Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses**

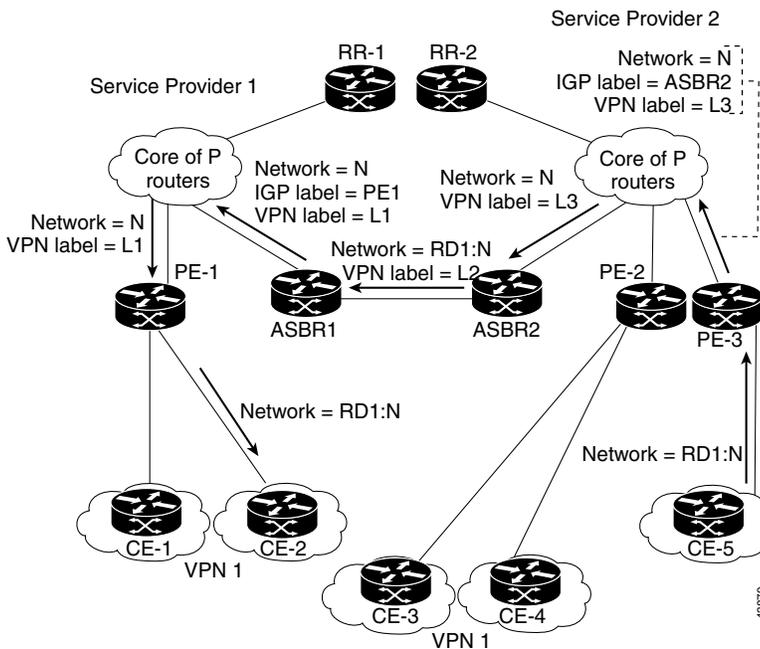
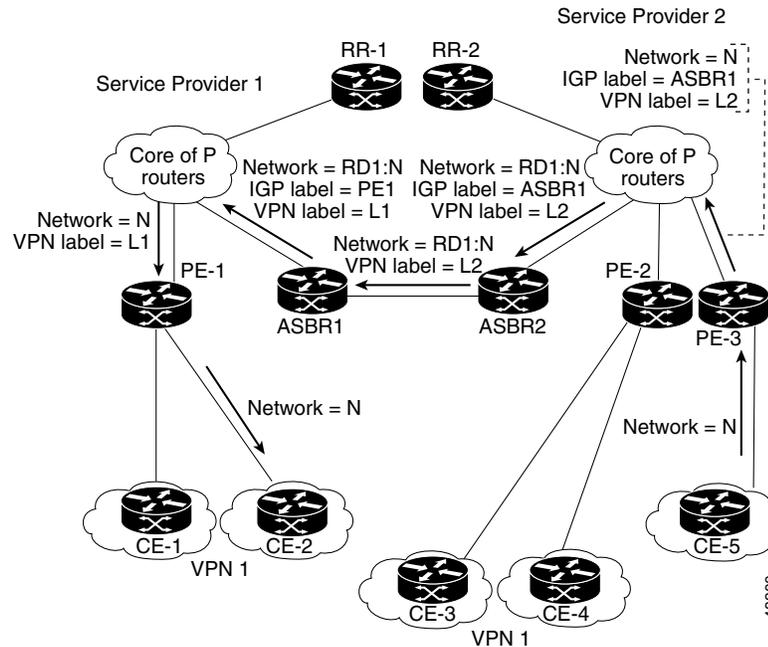


Figure 5 shows the same packet forwarding method, except the EBGP router (ASBR1) forwards the packet without reassigning it a new label.

**Figure 5 Forwarding Packets Without a New Label Assignment Between MPLS VPN Inter-AS System with ASBRs Exchanging VPN-IPv4 Addresses**



## Using a Confederation for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

A confederation is multiple subautonomous systems grouped together. 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. A VPN can span service providers running in separate autonomous systems or in multiple subautonomous systems that form a confederation.

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 either of 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.

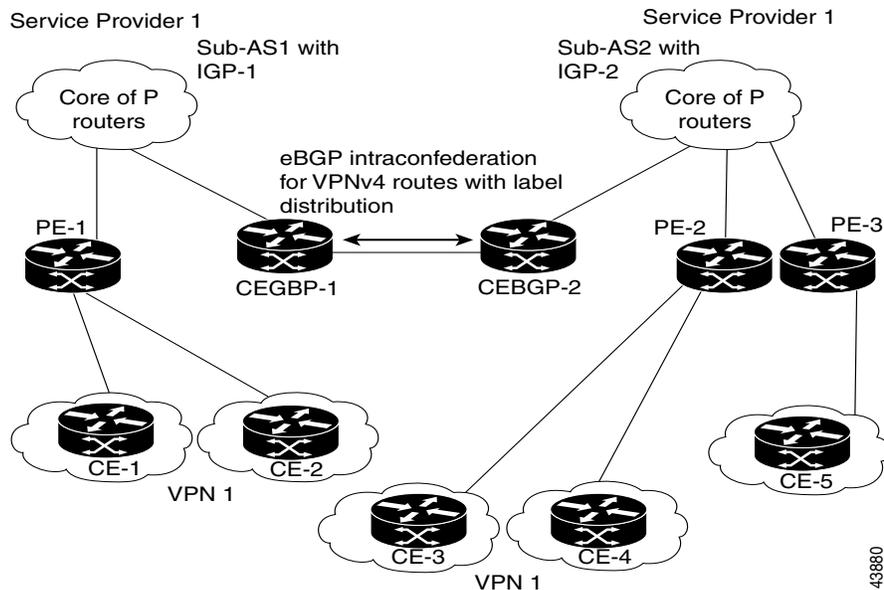
**Note**

Figure 2 and Figure 3 illustrate how two autonomous systems exchange routes and forward packets. Subautonomous systems in a confederation use a similar method of exchanging routes and forwarding packets.

Figure 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 6** *EBGP Connection Between Two Subautonomous Systems 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.

# How to Configure MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

To configure MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, perform the tasks in the following sections:

- [Configuring the ASBRs to Exchange VPN-IPv4 Addresses, page 11](#) (required)
- [Configuring EBGP Routing to Exchange VPN Routes Between Subautonomous Systems in a Confederation, page 12](#) (required)
- [Verifying Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 14](#) (optional)

## Configuring the ASBRs to Exchange VPN-IPv4 Addresses

To configure an EBGP ASBR to exchange VPN-IPv4 routes with another autonomous system, perform this task.



### Note

Issue the **redistribute connected subnets** command in the IGP configuration portion of the router to propagate host routes for VPN-IPv4 EBGP neighbors to other routers and provider edge routers. Alternatively, you can specify the next-hop-self address when you configure IBGP neighbors.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default route-target filter**
5. **address-family vpnv4** [*unicast*]
6. **neighbor** *peer-group-name* **remote-as** *as-number*
7. **neighbor** *peer-group-name* **activate**
8. **exit-address-family**
9. **end**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                             |
|--------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                   |

|        | Command or Action                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <code>router bgp as-number</code><br><br><b>Example:</b><br>Router(config)# router bgp 1                                                  | Creates an EBGP routing process and assigns it an AS number. The AS number is passed along and identifies the router to EBGP routers in another autonomous system.                                                                                                                                                                  |
| Step 4 | <code>no bgp default route-target filter</code><br><br><b>Example:</b><br>Router(config)# no bgp default route-target filter              | Disables BGP route-target filtering. All received BGP VPN-IPv4 routes are accepted by the router. Enters router configuration mode.                                                                                                                                                                                                 |
| Step 5 | <code>address-family vpnv4 [unicast]</code><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                         | Configures a routing session to carry VPNv4 addresses across the VPN backbone. Each address has been made globally unique by the addition of an 8-byte route distinguisher (RD). Enters address family configuration mode.<br><br><ul style="list-style-type: none"> <li>The unicast keyword specifies a unicast prefix.</li> </ul> |
| Step 6 | <code>neighbor peer-group-name remote-as as-number</code><br><br><b>Example:</b><br>Router(config-router-af)# neighbor Lowell remote-as 2 | Enters the address family submode and specifies a neighboring EBGP peer group. This EBGP peer group is identified to the specified autonomous system.                                                                                                                                                                               |
| Step 7 | <code>neighbor peer-group-name activate</code><br><br><b>Example:</b><br>Router(config-router-af)# neighbor Lowell activate               | Activates the advertisement of the VPNv4 address family to a neighboring EBGP router.                                                                                                                                                                                                                                               |
| Step 8 | <code>exit-address-family</code><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                  | Exits from the address family submode of the global configuration mode.                                                                                                                                                                                                                                                             |
| Step 9 | <code>end</code><br><br><b>Example:</b><br>Router(config)# end                                                                            | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                      |

## Configuring EBGP Routing to Exchange VPN Routes Between Subautonomous Systems in a Confederation

Perform this task to configure EBGP routing to exchange VPN routes between subautonomous systems in a confederation.



### Note

To ensure that the host routes for VPN-IPv4 EBGP neighbors are propagated (by means of the IGP) to the other routers and provider edge routers, specify the **redistribute connected** command in the IGP configuration portion of the CEBGP router. If you are using OSPF, make sure that the OSPF process is not enabled on the CEBGP interface where the “redistribute connected” subnet exists.

**Note**

In this confederation, subautonomous system IGP domains must know the addresses of CEBGP-1 and CEBGP-2. If you do not specify a next-hop-self address as part of the router configuration, ensure that the addresses of all PE routers in the subautonomous system are distributed throughout the network, not just the addresses of CEBGP-1 and CEBGP-2.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router bgp** *sub-autonomous-system*
4. **bgp confederation identifier** *as-number*
5. **bgp confederation peers** *sub-autonomous-system*
6. **no bgp default route-target filter**
7. **address-family vpnv4** [unicast]
8. **neighbor** *peer-group-name* **remote-as** *as-number*
9. **neighbor** *peer-group-name* **next-hop-self**
10. **neighbor** *peer-group-name* **activate**
11. **exit-address-family**
12. **end**

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                                    | <b>Purpose</b>                                                                                                                                                                                                        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                   |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                              | Enters global configuration mode.                                                                                                                                                                                     |
| <b>Step 3</b> | <b>router bgp</b> <i>sub-autonomous-system</i><br><br><b>Example:</b><br>Router(config)# router bgp 2                       | Creates an EBGp routing process and assigns it an AS number. The subautonomous system number is passed along to identify the router to EBGp routers in other subautonomous systems. Enters router configuration mode. |
| <b>Step 4</b> | <b>bgp confederation identifier</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# bgp confederation 100 | Defines an EBGp confederation by specifying a confederation identifier associated with each subautonomous system. The subautonomous systems appear as a single autonomous system.                                     |

|         | Command or Action                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <b>bgp confederation peers</b><br><i>sub-autonomous-system</i><br><br><b>Example:</b><br>Router(config-router)# bgp confederation<br>peers 1 | Specifies the subautonomous systems that belong to the confederation (identifies neighbors of other subautonomous systems within the confederation as special EBGp peers).                                                                                                                                                   |
| Step 6  | <b>no bgp default route-target filter</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default<br>route-target filter             | Disables BGP route-target community filtering. All received BGP VPN-IPv4 routes are accepted by the router.                                                                                                                                                                                                                  |
| Step 7  | <b>address-family vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router)# address-family<br>vpnv4                               | Configures a routing session to carry VPNv4 addresses across the VPN backbone. Each address has been made globally unique by the addition of an 8-byte route distinguisher (RD). Enters address family configuration mode. <ul style="list-style-type: none"> <li>The unicast keyword specifies a unicast prefix.</li> </ul> |
| Step 8  | <b>neighbor peer-group-name remote-as</b><br><i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor R<br>remote-as 1  | Enters the address family submode and specifies a neighboring EBGp peer group. This EBGp peer group is identified to the specified subautonomous system.                                                                                                                                                                     |
| Step 9  | <b>neighbor peer-group-name next-hop-self</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor R<br>next-hop-self                | Advertises the router as the next hop for the specified neighbor. If you specify a next-hop-self address as part of the router configuration, you do not need to use the <b>redistribute connected</b> command.                                                                                                              |
| Step 10 | <b>neighbor peer-group-name activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor R<br>activate                          | Activates the advertisement of the VPNv4 address family to a neighboring PE router in the specified subautonomous system.                                                                                                                                                                                                    |
| Step 11 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)#<br>exit-address-family                                        | Exits from the address family submode of the global configuration mode.                                                                                                                                                                                                                                                      |
| Step 12 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                     | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                               |

## Verifying Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Perform this task to display the VPN-IPv4 label forwarding information base (LFIB) entries.

## SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4** {all | rd *route-distinguisher* | vrf *vrf-name*} [summary] [labels]
3. **show mpls forwarding-table** [*network* {*mask* | *length*} | labels *label* [-*label*] | interface *interface* | next-hop *address* | lsp-tunnel [*tunnel-id*]] [vrf *vrf-name*] [detail]
4. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                    |
| Step 2 | <b>show ip bgp vpnv4</b> {all   rd <i>route-distinguisher</i>   vrf <i>vrf-name</i> } [summary] [labels]<br><br><b>Example:</b><br>Router# show ip bgp vpnv4 all labels                                                                                                                                           | Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>• Use the <b>all</b> and <b>labels</b> keywords to display information about all VPNv4 labels.</li> </ul> |
| Step 3 | <b>show mpls forwarding-table</b> [ <i>network</i> { <i>mask</i>   <i>length</i> }   labels <i>label</i> [- <i>label</i> ]   interface <i>interface</i>   next-hop <i>address</i>   lsp-tunnel [ <i>tunnel-id</i> ]] [vrf <i>vrf-name</i> ] [detail]<br><br><b>Example:</b><br>Router# show mpls forwarding-table | Displays the contents of the MPLS LFIB (such as VPNv4 prefix/length and BGP next-hop destination for the route).                                                                                      |
| Step 4 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                                                                          | Exits to user EXEC mode.                                                                                                                                                                              |

## Examples

The sample output of the **show mpls forwarding-table** command shows how the VPN-IPv4 LFIB entries appear:

```
Router# show mpls forwarding-table
```

```
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
33 33 10.120.4.0/24 0 Hs0/0 point2point
35 27 100:12:10.200.0.1/32 \
0 Hs0/0 point2point
```

In this example, the Prefix field appears as a VPN-IPv4 RD, plus the prefix. If the value is longer than the width of the Prefix column (as illustrated in the last line of the example), the output automatically wraps onto the next line in the forwarding table, preserving column alignment.

# Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Configuration examples for MPLS VPN Inter-AS include the following:

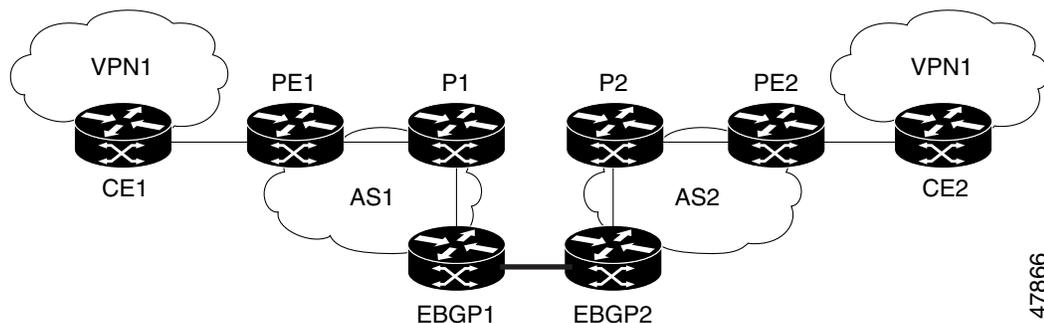
- [Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses: Example, page 16](#)
- [Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses in a Confederation: Example, page 23](#)

## Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses: Example

The network topology in [Figure 7](#) shows two autonomous systems, which are configured as follows:

- Autonomous system 1 (AS1) includes PE1, P1, and EBG1. The IGP is OSPF.
- Autonomous system 2 (AS2) includes PE2, P2, and EBG2. The IGP is ISIS.
- CE1 and CE2 belong to the same VPN, which is called VPN1.
- The P routers are route reflectors.
- EBG1 is configured with the **redistribute connected subnets** command.
- EBG2 is configured with the **neighbor next-hop-self** command.

**Figure 7** Configuring Two Autonomous Systems



### Configuration for Autonomous System 1, CE1 Example

The following example shows how to configure CE1 in VPN1 in a topology with two autonomous systems (see [Figure 7](#)):

```
CE1: Burlington
!
interface Loopback1
 ip address aa.0.0.6 255.255.255.255
!
interface Serial1/3
 description wychmere
 no ip address
 encapsulation frame-relay
```

```

frame-relay intf-type dce
!
interface Serial1/3.1 point-to-point
description wychmere
ip address aa.6.2.1 255.255.255.252
frame-relay interface-dlci 22
!
router ospf 1
network aa.0.0.0 0.255.255.255 area 0

```

## Configuration for Autonomous System 1, PE1 Example

The following example shows how to configure PE1 in AS1 in a topology with two autonomous systems (see [Figure 7](#)):

```

PE1: wychmere
!
ip cef
!
ip vrf V1
rd 1:105
route-target export 1:100
route-target import 1:100
!
interface Serial0/0
description Burlington
no ip address
encapsulation frame-relay
no fair-queue
clockrate 2000000
!
interface Serial0/0.3 point-to-point
description Burlington
ip vrf forwarding V1
ip address aa.6.2.2 255.255.255.252
frame-relay interface-dlci 22
!
interface Ethernet0/1
description Vermont
ip address aa.2.2.5 255.255.255.0
tag-switching ip
!
router ospf 1
log-adjacency-changes
network aa.0.0.0 0.255.255.255 area 0
!
router ospf 10 vrf V1
log-adjacency-changes
redistribute bgp 1 metric 100 subnets
network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
no synchronization
neighbor R peer-group
neighbor R remote-as 1
neighbor R update-source Loopback0
neighbor aa.0.0.2 peer-group R
no auto-summary
!
address-family ipv4 vrf V1
redistribute ospf 10
no auto-summary

```

```

no synchronization
exit-address-family
!
address-family vpnv4
neighbor R activate
neighbor R send-community extended
neighbor aa.0.0.2 peer-group R
no auto-summary
exit-address-family

```

## Configuration for Autonomous System 1, P1 Example

The following example shows how to configure P1 in AS1 in a topology with two autonomous systems (see [Figure 7](#)):

```

P1: Vermont
!
ip cef
!
interface Loopback0
 ip address aa.0.0.2 255.255.255.255
!
interface Ethernet0/1
 description Ogunquit
 ip address aa.2.1.1 255.255.255.0
 tag-switching ip
!
interface FastEthernet2/0
 description wychmere
 ip address aa.2.2.1 255.255.255.0
 duplex auto
 speed auto
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor aa.0.0.4 peer-group R
 neighbor aa.0.0.5 peer-group R
!
address-family vpnv4
 neighbor R activate
 neighbor R route-reflector-client
 neighbor R send-community extended
 neighbor aa.0.0.4 peer-group R
 neighbor aa.0.0.5 peer-group R
exit-address-family

```

## Configuration for Autonomous System 1, EBGPI Example

The following example shows how to configure EBGPI in AS1 in a topology with two autonomous systems (see [Figure 7](#)):

```

EBGP1: Ogunquit
!
ip cef
!
interface Loopback0
 ip address aa.0.0.4 255.255.255.255
!
EBGP1: Ogunquit
!
ip cef
!
interface Loopback0
 ip address aa.0.0.4 255.255.255.255
!
interface Ethernet0/1
 description Vermont
 ip address aa.2.1.40 255.255.255.0
 tag-switching ip
!
interface ATM1/0
 description Lowell
 no ip address
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 description Lowell
 ip address aa.0.0.1 255.255.255.252
 pvc 1/100
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor aa.0.0.2 remote-as 2
 neighbor aa.0.0.2 peer-group R
 no auto-summary
!
address-family vpnv4
 neighbor R activate
 neighbor R send-community extended
 neighbor aa.0.0.2 activate
 neighbor aa.0.0.2 send-community extended
 neighbor aa.0.0.2 peer-group R
 no auto-summary
 exit-address-family

```

## Configuration for Autonomous System 2, EBG2 Example

The following example shows how to configure EBG2 in AS2 in a topology with two autonomous systems (see [Figure 7](#)):

```

EBGP2: Lowell
!

```

```

ip cef
!
ip vrf V1
 rd 2:103
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address aa.0.0.3 255.255.255.255
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address aa.0.0.3 255.255.255.255
!
interface Serial0/0
 description Littleton
 no ip address
 encapsulation frame-relay
 load-interval 30
 no fair-queue
 clockrate 2000000
!
interface Serial0/0.2 point-to-point
 description Littleton
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
interface ATM1/0
 description Ogunquit
 no ip address
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 description Ogunquit
 ip address aa.0.0.2 255.255.255.252
 pvc 1/100
!
router isis
 net 49.0002.0000.0000.0003.00
!
router bgp 2
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor aa.0.0.1 remote-as 1
 neighbor aa.0.0.8 remote-as 2
 neighbor aa.0.0.8 update-source Loopback0
 neighbor aa.0.0.8 next-hop-self
!
 address-family ipv4 vrf V1
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor aa.0.0.1 activate
 neighbor aa.0.0.1 send-community extended
 neighbor aa.0.0.8 activate

```

```

neighbor aa.0.0.8 next-hop-self
neighbor aa.0.0.8 send-community extended
exit-address-family

```

## Configuration for Autonomous System 2, P2 Example

The following example shows how to configure P2 in AS2 in a topology with two autonomous systems (see [Figure 7](#)):

```

P2: Littleton
!
ip cef
!
ip vrf V1
 rd 2:108
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address aa.0.0.8 255.255.255.255
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address aa.0.0.8 255.255.255.255
!
interface FastEthernet0/0
 description Pax
 ip address aa.9.1.2 255.255.255.0
 ip router isis
 tag-switching ip
!
interface Serial5/0
 description Lowell
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface Serial5/0.1 point-to-point
 description Lowell
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
router isis
 net aa.0002.0000.0000.0008.00
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 2
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor aa.0.0.3 peer-group R
 neighbor aa.0.0.9 peer-group R
!
address-family ipv4 vrf V1
 redistribute connected
 no auto-summary
 no synchronization

```

```

 exit-address-family
 !
 address-family vpnv4
 neighbor R activate
 neighbor R route-reflector-client
 neighbor R send-community extended
 neighbor aa.0.0.3 peer-group R
 neighbor aa.0.0.9 peer-group R
 exit-address-family

```

## Configuration for Autonomous System 2, PE2 Example

The following example shows how to configure PE2 in AS2 in a topology with two autonomous systems (see [Figure 7](#)):

```

PE2: Pax
!
ip cef
!
ip vrf V1
 rd 2:109
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address aa.0.0.9 255.255.255.255
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address aa.0.0.9 255.255.255.255
!
interface Serial0/0
 description Bethel
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 no fair-queue
 clockrate 2000000
!
interface Serial0/0.1 point-to-point
 description Bethel
 ip vrf forwarding V1
 ip unnumbered Loopback1
 frame-relay interface-dlci 24
!
interface FastEthernet0/1
 description Littleton
 ip address aa.9.1.1 255.255.255.0
 ip router isis
 tag-switching ip
!
router ospf 10 vrf V1
 log-adjacency-changes
 redistribute bgp 2 subnets
 network aa.0.0.0 0.255.255.255 area 0
!
router isis
 net 49.0002.0000.0000.0009.00
!
router bgp 2
 no synchronization

```

```

bgp log-neighbor-changes
neighbor aa.0.0.8 remote-as 2
neighbor aa.0.0.8 update-source Loopback0
!
address-family ipv4 vrf V1
 redistribute connected
 redistribute ospf 10
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpnv4
 neighbor aa.0.0.8 activate
 neighbor aa.0.0.8 send-community extended
 exit-address-family v

```

## Configuration for Autonomous System 2, CE2 Example

The following example shows how to configure CE2 in VPN1 in a topology with two autonomous systems (see [Figure 7](#)):

```

CE2: Bethel
!
interface Loopback0
 ip address 1.0.0.11 255.255.255.255
!
interface Serial0
 description Pax
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
!
interface Serial0.1 point-to-point
 description Pax
 ip unnumbered Loopback0
 frame-relay interface-dlci 24
!
router ospf 1
 network aa.0.0.0 0.255.255.255 area 0

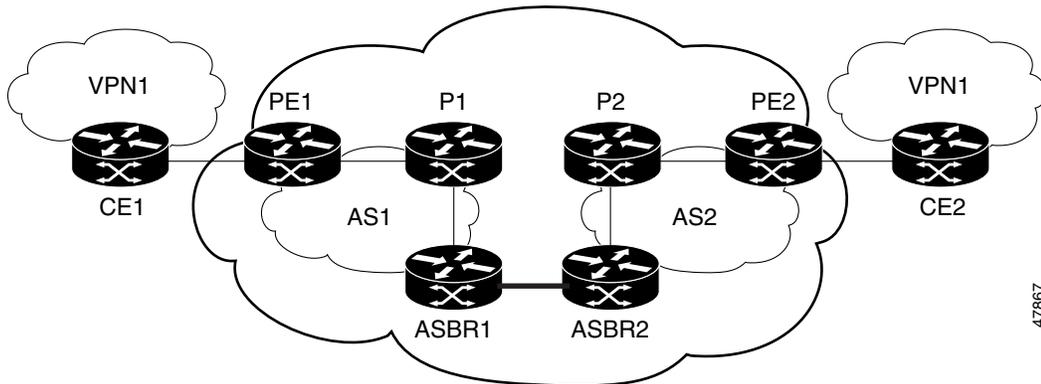
```

## Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses in a Confederation: Example

The network topology in [Figure 8](#) shows a single Internet service provider (ISP), which is partitioning the backbone with confederations. The AS number of the provider is 100. The two autonomous systems run their own IGP and are configured as follows:

- Autonomous system 1 (AS1) includes PE1, P1, CEBGP1. The IGP is OSPF.
- Autonomous system 2 (AS2) includes PE2, P2, CEBGP2. The IGP is ISIS.
- CE1 and CE2 belong to the same VPN, which is called VPN1.
- The P routers are route reflectors.
- CEBGP1 is configured with the **redistribute connected subnets** command.
- CEBGP2 is configured with the **neighbor next-hop-self** command.

**Figure 8** Configuring Two Autonomous Systems in a Confederation



47867

## Configuration for Autonomous System 1, CE1 Example

The following example shows how to configure CE1 in VPN1 in a confederation topology (see [Figure 8](#)):

```
CE1: Burlington
!
interface Loopback1
 ip address aa.0.0.6 255.255.255.255
!
interface Serial1/3
 description wychmere
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface Serial1/3.1 point-to-point
 description wychmere
 ip address aa.6.2.1 255.255.255.252
 frame-relay interface-dlci 22
!
router ospf 1
 network aa.0.0.0 0.255.255.255 area 0
```

## Configuration for Autonomous System 1, PE1 Example

The following example shows how to configure PE1 in AS1 in a confederation topology (see [Figure 8](#)):

```
PE1: wychmere
!
ip cef
!
ip vrf V1
 rd 1:105
 route-target export 1:100
 route-target import 1:100
!
interface Serial0/0
 description Burlington
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
```

```

!
interface Serial0/0.3 point-to-point
 description Burlington
 ip vrf forwarding V1
 ip address aa.6.2.2 255.255.255.252
 frame-relay interface-dlci 22
!
interface Ethernet0/1
 description Vermont
 ip address aa.2.2.5 255.255.255.0
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network aa.0.0.0 0.255.255.255 area 0
!
router ospf 10 vrf V1
 log-adjacency-changes
 redistribute bgp 1 metric 100 subnets
 network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
 no synchronization
 bgp confederation identifier 100
 bgp confederation identifier 100
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor aa.0.0.2 peer-group R
 no auto-summary
!
 address-family ipv4 vrf V1
 redistribute ospf 10
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor R activate
 neighbor R send-community extended
 neighbor aa.0.0.2 peer-group R
 no auto-summary
 exit-address-family

```

## Configuration for Autonomous System 1, P1 Example

The following example shows how to configure P1 in AS1 in a confederation topology (see [Figure 8](#)):

```

P1: Vermont
!
ip cef
!
interface Loopback0
 ip address aa.0.0.2 255.255.255.255
!
interface Ethernet0/1
 description Ogunquit
 ip address 100.2.1.1 255.255.255.0
 tag-switching ip
!
interface FastEthernet2/0

```

```

description wychmere
ip address aa.2.2.1 255.255.255.0
duplex auto
speed auto
tag-switching ip
!
router ospf 1
log-adjacency-changes
network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 100
neighbor R peer-group
neighbor R remote-as 1
neighbor R update-source Loopback0
neighbor R route-reflector-client
neighbor 100.0.0.4 peer-group R
neighbor 100.0.0.5 peer-group R
!
address-family vpnv4
neighbor R activate
neighbor R route-reflector-client
neighbor R send-community extended
neighbor aa.0.0.4 peer-group R
neighbor aa.0.0.5 peer-group R
exit-address-family

```

## Configuration for Autonomous System 1, CEBGP1 Example

The following example shows how to configure CEBGP1 in AS1 in a confederation topology (see [Figure 8](#)):

```

EBGP1: Ogunquit
!
ip cef
!
interface Loopback0
ip address aa.0.0.4 255.255.255.255
!
interface Ethernet0/1
description Vermont
ip address aa.2.1.40 255.255.255.0
tag-switching ip
!
interface ATM1/0
description Lowell
no ip address
no atm scrambling cell-payload
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
description Lowell
ip address aa.0.0.1 255.255.255.252
pvc 1/100
!
router ospf 1
log-adjacency-changes
redistribute connected subnets
network aa.0.0.0 0.255.255.255 area 0
!

```

```

router bgp 1
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 bgp confederation identifier 100
 bgp confederation peers 1
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor aa.0.0.2 remote-as 2
 neighbor aa.0.0.2 next-hop-self
 neighbor aa.0.0.2 peer-group R
 no auto-summary
 !
 address-family vpnv4
 neighbor R activate
 neighbor R send-community extended
 neighbor aa.0.0.2 activate
 neighbor aa.0.0.2 next-hop-self
 neighbor aa.0.0.2 send-community extended
 neighbor aa.0.0.2 peer-group R
 no auto-summary
 exit-address-family

```

## Configuration for Autonomous System 2, CEBGP2 Example

The following example shows how to configure CEBGP2 in AS2 in a confederation topology (see [Figure 8](#)):

```

EBGP2: Lowell
!
ip cef
!
ip vrf V1
 rd 2:103
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address aa.0.0.3 255.255.255.255
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address aa.0.0.3 255.255.255.255
!
interface Serial0/0
 description Littleton
 no ip address
 encapsulation frame-relay
 load-interval 30
 no fair-queue
 clockrate 2000000
!
interface Serial0/0.2 point-to-point
 description Littleton
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
interface ATM1/0

```

```

description Ogunquit
no ip address
atm clock INTERNAL
no atm scrambling cell-payload
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
description Ogunquit
ip address aa.0.0.2 255.255.255.252
pvc 1/100
!
router isis
net aa.0002.0000.0000.0003.00
!
router bgp 2
no synchronization
no bgp default route-target filter
bgp log-neighbor-changes
bgp confederation identifier 100
bgp confederation peers 1
neighbor aa.0.0.1 remote-as 1
neighbor aa.0.0.1 next-hop-self
neighbor aa.0.0.8 remote-as 2
neighbor aa.0.0.8 update-source Loopback0
neighbor aa.0.0.8 next-hop-self
!
address-family ipv4 vrf V1
redistribute connected
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor aa.0.0.1 activate
neighbor aa.0.0.1 next-hop-self
neighbor aa.0.0.1 send-community extended
neighbor aa.0.0.8 activate
neighbor aa.0.0.8 next-hop-self
neighbor aa.0.0.8 send-community extended
exit-address-family

```

## Configuration for Autonomous System 2, P2 Example

The following example shows how to configure P2 in AS2 in a confederation topology (see [Figure 8](#)):

```

P2: Littleton
!
ip cef
!
ip vrf V1
rd 2:108
route-target export 1:100
route-target import 1:100
!
interface Loopback0
ip address aa.0.0.8 255.255.255.255
ip router isis
!
interface Loopback1
ip vrf forwarding V1
ip address aa.0.0.8 255.255.255.255

```

```

!
interface FastEthernet0/0
 description Pax
 ip address aa.9.1.2 255.255.255.0
 ip router isis
 tag-switching ip
!
interface Serial5/0
 description Lowell
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface Serial5/0.1 point-to-point
 description Lowell
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
router isis
 net aa.0002.0000.0000.0008.00
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 bgp confederation identifier 100
 neighbor R peer-group
 neighbor R remote-as 2
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor aa.0.0.3 peer-group R
 neighbor aa.0.0.9 peer-group R
!
address-family ipv4 vrf V1
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpnv4
 neighbor R activate
 neighbor R route-reflector-client
 neighbor R send-community extended
 neighbor aa.0.0.3 peer-group R
 neighbor aa.0.0.9 peer-group R
 exit-address-family

```

## Configuration for Autonomous System 2, PE2 Example

The following example shows how to configure PE2 in AS2 in a confederation topology (see [Figure 8](#)):

```

PE2: Pax
!
ip cef
!
ip vrf V1
 rd 2:109
 route-target export 1:100
 route-target import 1:100
!

```

```

interface Loopback0
 ip address aa.0.0.9 255.255.255.255
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address 1.0.0.9 255.255.255.255
!
interface Serial0/0
 description Bethel
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 no fair-queue
 clockrate 2000000
!
interface Serial0/0.1 point-to-point
 description Bethel
 ip vrf forwarding V1
 ip unnumbered Loopback1
 frame-relay interface-dlci 24
!
interface FastEthernet0/1
 description Littleton
 ip address 200.9.1.1 255.255.255.0
 ip router isis
 tag-switching ip
!
router ospf 10 vrf V1
 log-adjacency-changes
 redistribute bgp 2 subnets
 network aa.0.0.0 0.255.255.255 area 0
!
router isis
 net aa.0002.0000.0000.0009.00
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 bgp confederation identifier 100
 neighbor aa.0.0.8 remote-as 2
 neighbor aa.0.0.8 update-source Loopback0
!
 address-family ipv4 vrf V1
 redistribute connected
 redistribute ospf 10
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor aa.0.0.8 activate
 neighbor aa.0.0.8 send-community extended
 exit-address-family

```

## Configuration for Autonomous System 2, CE2 Example

The following example shows how to configure CE2 in VPN1 in a confederation topology (see [Figure 8](#)):

```

CE2: Bethel
!

```

```
interface Loopback0
 ip address aa.0.0.11 255.255.255.255
!
interface Serial0
 description Pax
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
!
interface Serial0.1 point-to-point
 description Pax
 ip unnumbered Loopback0
 frame-relay interface-dlci 24
!
router ospf 1
 network aa.0.0.0 0.255.255.255 area 0
```

## Additional References

The following sections provide references related to MPLS VPNs.

### Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC      | Title                                                         |
|----------|---------------------------------------------------------------|
| RFC 1700 | <i>Assigned Numbers</i>                                       |
| RFC 1966 | <i>BGP Route Reflection: An Alternative to Full Mesh IBGP</i> |
| RFC 2842 | <i>Capabilities Advertisement with BGP-4</i>                  |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>                     |
| RFC 3107 | <i>Carrying Label Information in BGP-4</i>                    |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

[Table 2](#) lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

[Table 2](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

| Feature Name                            | Releases                                          | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Interautonomous System Support | 12.1(5)T<br>12.0(16)ST<br>12.0(17)ST<br>12.0(22)S | This feature enables an MPLS VPN to span service providers and autonomous systems. This feature explains how to configuring the Inter-AS using the ASBRs to exchange VPN-IPv4 Addresses.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">Information about Using Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 4</a></li> <li><a href="#">How to Configure MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 11</a></li> </ul> |

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

---

The MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels feature allows an MPLS VPN to span service providers and autonomous systems. This module explains how to configure an MPLS VPN Inter-AS network so that the Autonomous System Boundary Routers (ASBRs) exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPN-IPv4 routes by using multihop, multiprotocol, External Border Gateway Protocol (eBGP).

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels”](#) section on page 38.

## Contents

- [Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 2](#)
- [Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 2](#)
- [Information About MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 3](#)
- [How to Configure MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 6](#)
- [Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 20](#)
- [Additional References, page 36](#)
- [Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 38](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

The network must be properly configured for MPLS VPN operation before you configure this feature.

[Table 1](#) lists the Cisco 12000 series line card support added by Cisco IOS S releases.

**Table 1** Cisco 12000 Series Line Card Support Added for Cisco IOS S Releases

| Type                             | Line Cards                                                                                                                                                                                                                               | Cisco IOS Release Supported                         |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Packet Over SONET (POS)          | 4-Port OC-3 POS<br>8-Port OC-3 POS<br>16-Port OC-3 POS<br>1-Port OC-12 POS<br>4-Port OC-12 POS<br>1-Port OC-48 POS<br>4-Port OC-3 POS ISE<br>8-Port OC-3 POS ISE<br>16-Port OC-3 POS ISE<br>4-Port OC-12 POS ISE<br>1-Port OC-48 POS ISE | 12.0(22)S, 12.0(23)S,<br>12.0(27)S                  |
| Electrical Interface             | 6-Port DS3<br>12-Port DS3<br>6-Port E3<br>12-Port E3                                                                                                                                                                                     | 12.0(22)S, 12.0(23)S,<br>12.0(27)S                  |
| Ethernet                         | 3-Port GbE                                                                                                                                                                                                                               | 12.0(23)S, 12.0(27)S                                |
| Asynchronous Transfer Mode (ATM) | 4-Port OC-3 ATM<br>1-Port OC-12 ATM<br>4-Port OC-12 ATM<br>8-Port OC-3 ATM                                                                                                                                                               | 12.0(22)S, 12.0(23)S,<br>12.0(27)S<br><br>12.0(23)S |
| Channelized Interface            | 2-Port CHOC-3<br>6-Port Ch T3 (DS1)<br>1-Port CHOC-12 (DS3)<br>1-Port CHOC-12 (OC-3)<br>4-Port CHOC-12 ISE<br>1-Port CHOC-48 ISE                                                                                                         | 12.0(22)S, 12.0(23)S,<br>12.0(27)S                  |

## Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

This feature includes the following restrictions:

- For networks configured with eBGP multihop, you must configure a label switched path (LSP) between nonadjacent routers. (RFC 3107)
- The physical interfaces that connect the BGP speakers must support Cisco Express Forwarding (CEF) or distributed CEF and MPLS.

# Information About MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

Before configuring MPLS VPN Inter-AS, you should understand the following concepts:

- [MPLS VPN Inter-AS Introduction, page 3](#)
- [Benefits of MPLS VPN Inter-AS, page 3](#)
- [Information About Using MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 4](#)
- [Benefits of MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 4](#)
- [How the Inter-AS Works When ASBRs Exchange IPv4 Routes with MPLS Labels, page 4](#)

## MPLS VPN Inter-AS Introduction

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.

## Benefits of MPLS VPN Inter-AS

This feature provides the following benefits.

- Allows a VPN to cross more than one service provider backbone

Service providers, running separate autonomous systems, can 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. This feature allows multiple autonomous systems to form a continuous (and seamless) network between customer sites of a service provider.

- Allows a VPN to exist in different areas

A service provider can 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

Internal Border Gateway Protocol (iBGP) meshing in an autonomous system is 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 (NLRI) between the subautonomous systems that form the confederation.

## Information About Using MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

You can set up the MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPN-IPv4 routes by using multihop, multiprotocol, External Border Gateway Protocol (eBGP). This method of configuring the Inter-AS system is often called MPLS VPN Inter-AS—IPv4 BGP Label Distribution.

## Benefits of MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

Configuring the Inter-AS system so that the ASBRs exchange the IPv4 routes and MPLS labels has the following benefits:

- Saves the ASBRs from having to store all the VPN-IPv4 routes. Using the route reflectors to store the VPN-IPv4 routes and forward them to the PE routers results in improved scalability compared with configurations where the ASBR holds all of the VPN-IPv4 routes and forwards the routes based on VPN-IPv4 labels.
- Having the route reflectors hold the VPN-IPv4 routes also simplifies the configuration at the border of the network.
- Enables a non-VPN core network to act as a transit network for VPN traffic—You can transport IPv4 routes with MPLS labels over a non-MPLS VPN service provider.
- Eliminates the need for any other label distribution protocol between adjacent LSRs—If two adjacent label switch routers (LSRs) are also BGP peers, BGP can handle the distribution of the MPLS labels. No other label distribution protocol is needed between the two LSRs.

## How the Inter-AS Works When ASBRs Exchange IPv4 Routes with MPLS Labels

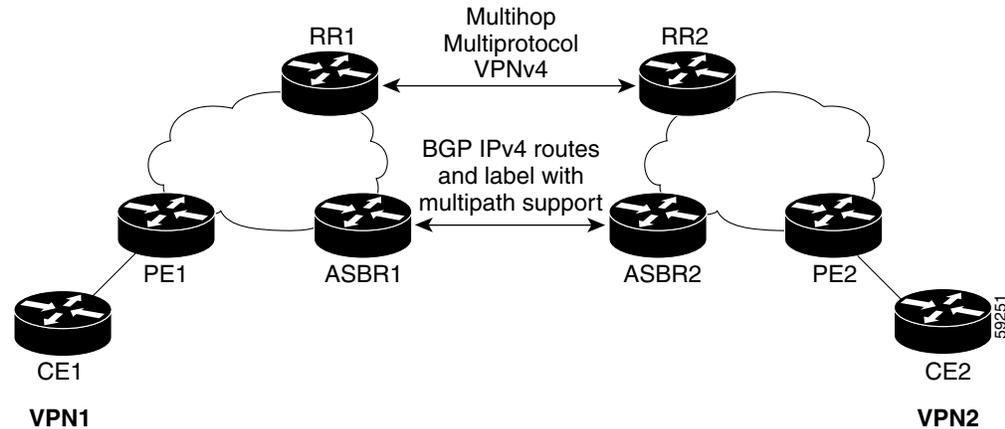
You can set up a VPN service provider network to exchange IPv4 routes with MPLS labels. You can configure the VPN service provider network as follows:

- Route reflectors exchange VPN-IPv4 routes by using multihop, multiprotocol eBGP. This configuration also preserves the next-hop information and the VPN labels across the autonomous systems.
- A local PE router (for example, PE1 in [Figure 1](#)) needs to know the routes and label information for the remote PE router (PE2). This information can be exchanged between the PE routers and ASBRs in one of two ways:
  - **Internal Gateway Protocol (IGP) and Label Distribution Protocol (LDP):** The ASBR can redistribute the IPv4 routes and MPLS labels it learned from eBGP into IGP and LDP and vice versa.
  - **Internal Border Gateway Protocol (iBGP) IPv4 label distribution:** The ASBR and PE router can use direct iBGP sessions to exchange VPN-IPv4 and IPv4 routes and MPLS labels.

Alternatively, the route reflector can reflect the IPv4 routes and MPLS labels learned from the ASBR to the PE routers in the VPN. This is accomplished by enabling the ASBR to exchange IPv4 routes and MPLS labels with the route reflector. The route reflector also reflects the VPN-IPv4 routes to the PE routers in the VPN. For example, in VPN1, RR1 reflects to PE1 the

VPN-IPv4 routes it learned and IPv4 routes and MPLS labels learned from ASBR1. Using the route reflectors to store the VPN-IPv4 routes and forward them through the PE routers and ASBRs allows for a scalable configuration.

**Figure 1** *VPNs Using eBGP and iBGP to Distribute Routes and MPLS Labels*



## BGP Routing Information

BGP routing information includes the following items:

- A network number (prefix), which is the IP address of the destination.
- Autonomous system (AS) path, which is a list of the other ASs through which a route passes on its way to the local router. The first AS in the list is closest to the local router; the last AS in the list is farthest from the local router and usually the AS where the route began.
- Path attributes, which provide other information about the AS path, for example, the next hop.

## Types of BGP Messages and MPLS Labels

MPLS labels are included in the update messages that a router sends. Routers exchange the following types of BGP messages:

- Open messages—After a router establishes a TCP connection with a neighboring router, the routers exchange open messages. This message contains the number of the AS to which the router belongs and the IP address of the router who sent the message.
- Update messages—When a router has a new, changed, or broken route, it sends an update message to the neighboring router. This message contains the NLRI, which lists the IP addresses of the usable routes. The update message includes any routes that are no longer usable. The update message also includes path attributes and the lengths of both the usable and unusable paths. Labels for VPN-IPv4 routes are encoded in the update message as specified in RFC 2858. The labels for the IPv4 routes are encoded in the update message as specified in RFC 3107.
- Keepalive messages—Routers exchange keepalive messages to determine if a neighboring router is still available to exchange routing information. The router sends these messages at regular intervals. (Sixty seconds is the default for Cisco routers.) The keepalive message does not contain routing data; it only contains a message header.
- Notification messages—When a router detects an error, it sends a notification message.

## How BGP Sends MPLS Labels with Routes

When BGP (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.

When you issue the **neighbor send-label** command on both BGP routers, the routers advertise to each other that they can then send MPLS labels with the routes. If the routers successfully negotiate their ability to send MPLS labels, the routers add MPLS labels to all outgoing BGP updates.

## How to Configure MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

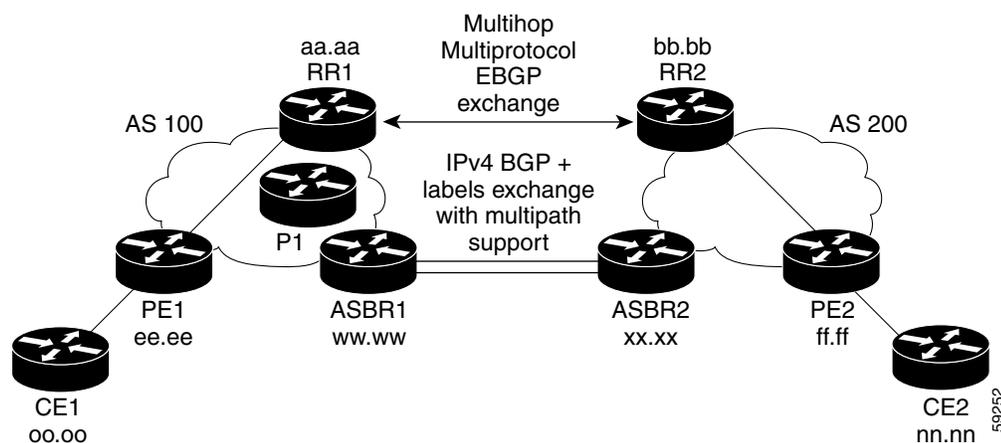
To configure MPLS VPN Inter-AS with ASBRs exchanging IPv4 routes and MPLS labels, perform the tasks in the following sections:

- [Configuring the ASBRs to Exchange IPv4 Routes and MPLS Labels, page 6](#)
- [Configuring the Route Reflectors to Exchange VPN-IPv4 Routes, page 8](#)
- [Configuring the Route Reflector to Reflect Remote Routes in Its AS, page 10](#)
- [Verifying the MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels Configuration, page 13](#)

Figure 2 shows the following sample configuration:

- The configuration consists of two VPNs.
- The ASBRs exchange the IPv4 routes with MPLS labels.
- The route reflectors exchange the VPN-IPv4 routes using multihop MPLS eBGP.
- The route reflectors reflect the IPv4 and VPN-IPv4 routes to the other routers in its AS.

**Figure 2** Configuring Two VPN Service Providers to Exchange IPv4 Routes and MPLS Labels



## Configuring the ASBRs to Exchange IPv4 Routes and MPLS Labels

Perform this task to configure the ASBRs to exchange IPv4 routes and MPLS labels. This configuration procedure uses ASBR1 as an example.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** *ip-address* **send-label**
8. **exit-address-family**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                             | Configures a BGP routing process and places the router in router configuration mode.<br><ul style="list-style-type: none"><li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li></ul> |
| Step 4 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor hh.0.0.1<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table.<br><ul style="list-style-type: none"><li>• The <i>ip-address</i> argument specifies the IP address of the neighbor.</li><li>• The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li><li>• The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li></ul>                                                                  |

|        | Command or Action                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p><b>address-family ipv4</b> [<b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4</p>   | <p>Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv4 address prefixes.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VPN routing/forwarding instance (VRF) to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 6 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}</p> <p><b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor hh.0.0.1 activate</p> | <p>Enables the exchange of information with a neighboring router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                 |
| Step 7 | <p><b>neighbor</b> <i>ip-address</i> <b>send-label</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor hh.0.0.1 send-label</p>                               | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                                                                                                                                                                                     |
| Step 8 | <p><b>exit-address-family</b></p> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                                 | <p>Exits from the address family configuration submode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 9 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                                 | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Configuring the Route Reflectors to Exchange VPN-IPv4 Routes

Perform this task to enable the route reflectors to exchange VPN-IPv4 routes by using multihop, multiprotocol eBGP.

This procedure also specifies that the next hop information and the VPN label are to be preserved across the autonomous systems. This procedure uses RR1 as an example of the route reflector.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*

5. **address-family vpnv4 [unicast]**
6. **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*tll*]
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **next-hop unchanged**
9. **exit-address-family**
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                                | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> <p>The AS number identifies RR1 to routers in other autonomous systems.</p> |
| Step 4 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor bb.bb.bb.bb<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                |
| Step 5 | <b>address-family vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                                                | Enters address family configuration mode for configuring routing sessions, such as BGP sessions, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                                                                                                                                         |

|         | Command or Action                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>ebgp-multihop</b> [ <i>ttl</i> ]<br><br><b>Example:</b><br>Router(config-router-af)# neighbor bb.bb.bb.bb<br>ebgp-multihop 255 | Accepts and attempts BGP connections to external peers residing on networks that are not directly connected. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>ttl</i> argument specifies the time-to-live in the range from 1 to 255 hops.</li> </ul> |
| Step 7  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor bb.bb.bb.bb<br>activate                              | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                         |
| Step 8  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>next-hop unchanged</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor ip-address<br>next-hop unchanged           | Enables an External BGP (eBGP) multihop peer to propagate the next hop unchanged. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the next hop.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group that is the next hop.</li> </ul>                                                                                                                 |
| Step 9  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                                  | Exits from the address family configuration submode.                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                                     | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                              |

## Configuring the Route Reflector to Reflect Remote Routes in Its AS

Perform this task to enable the RR to reflect the IPv4 routes and labels learned by the ASBR to the PE routers in the AS.

This is accomplished by making the ASBR and PE router route reflector clients of the RR. This procedure also explains how to enable the RR to reflect the VPN-IPv4 routes.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **activate**

6. **neighbor** *ip-address* **route-reflector-client**
7. **neighbor** *ip-address* **send-label**
8. **exit-address-family**
9. **address-family** **vpn**v4 [**unicast**]
10. **neighbor** {*ip-address* | *peer-group-name*} **activate**
11. **neighbor** *ip-address* **route-reflector-client**
12. **exit-address-family**
13. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>router</b> <b>bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                        | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                        |
| Step 4 | <b>address-family</b> <b>ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 | Enters address family configuration mode for configuring routing sessions, such as BGP sessions, that use standard IPv4 address prefixes. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VPN routing and forwarding instance (VRF) to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |

|         | Command or Action                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor ee.ee.ee.ee<br/>activate</p>          | <p>Enables the exchange of information with a neighboring router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 6  | <pre>neighbor ip-address route-reflector-client</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor ee.ee.ee.ees<br/>route-reflector-client</p> | <p>Configures the router as a BGP route reflector and configures the specified neighbor as its client.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP neighbor being configured as a client.</li> </ul>                |
| Step 7  | <pre>neighbor ip-address send-label</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor ee.ee.ee.ee<br/>send-label</p>                          | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                     |
| Step 8  | <pre>exit-address-family</pre> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                     | <p>Exits from address family configuration submenu.</p>                                                                                                                                                                                                                               |
| Step 9  | <pre>address-family vpnv4 [unicast]</pre> <p><b>Example:</b><br/>Router(config-router)# address-family vpnv4</p>                                            | <p>Enters address family configuration mode for configuring routing sessions, such as BGP sessions, that use standard VPNv4 address prefixes.</p> <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>     |
| Step 10 | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor ee.ee.ee.ee<br/>activate</p>          | <p>Enables the exchange of information with a neighboring router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 11 | <pre>neighbor ip-address route-reflector-client</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor ee.ee.ee.ee<br/>route-reflector-client</p>  | <p>Enables the RR to pass iBGP routes to the neighboring router.</p>                                                                                                                                                                                                                  |
| Step 12 | <pre>exit-address-family</pre> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                     | <p>Exits from the address family configuration submenu.</p>                                                                                                                                                                                                                           |
| Step 13 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                     | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                      |

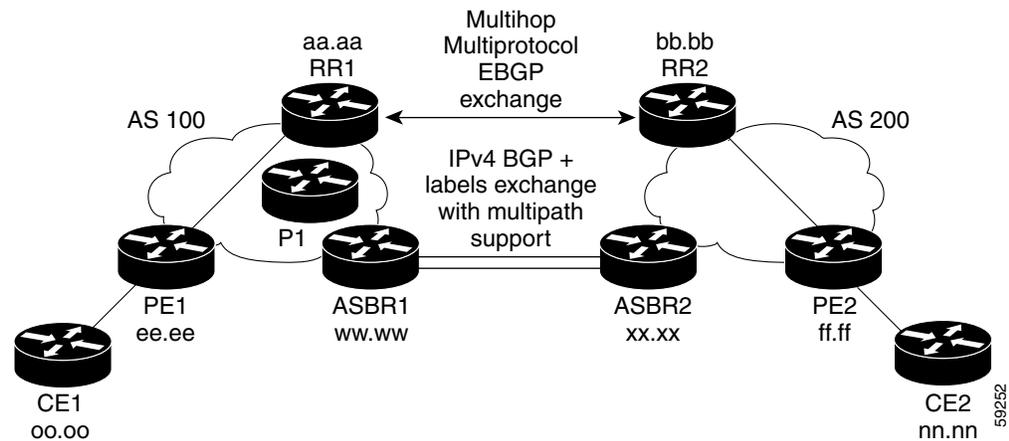
## Verifying the MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels Configuration

If you use ASBRs to distribute the IPv4 labels and route reflectors to distribute the VPN-IPv4 routes, use the following procedures to help verify the configuration:

- [Verifying the Route Reflector Configuration, page 13](#)
- [Verifying that CE1 Can Communicate with CE2, page 14](#)
- [Verifying that PE1 Can Communicate with CE2, page 15](#)
- [Verifying that PE2 Can Communicate with CE2, page 17](#)
- [Verifying the ASBR Configuration, page 18](#)

Figure 3 shows the configuration that is referred to in the next several sections.

**Figure 3** Configuring Two VPN Service Providers to Exchange IPv4 Routes and MPLS Labels



### Verifying the Route Reflector Configuration

Perform this task to verify the route reflector configuration.

#### SUMMARY STEPS

1. `enable`
2. `show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [summary] [labels]`
3. `disable`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                  | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <p><b>show ip bgp vpnv4</b> {<b>all</b>   <b>rd</b> <i>route-distinguisher</i>   <b>vrf</b> <i>vrf-name</i>} [<b>summary</b>] [<b>labels</b>]</p> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 all summary</p> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 all labels</p> | <p>(Optional) Displays VPN address information from the BGP table.</p> <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>summary</b> keywords to verify that a multihop, multiprotocol eBGP session exists between the route reflectors and that the VPNv4 routes are being exchanged between the route reflectors.</li> </ul> <p>The last two lines of the command output show the following information:</p> <ul style="list-style-type: none"> <li>Prefixes are being learned from PE1 and then passed to RR2.</li> <li>Prefixes are being learned from RR2 and then passed to PE1.</li> </ul> <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>labels</b> keywords to verify that the route reflectors exchange VPNv4 label information.</li> </ul> |
| Step 3 | <p><b>disable</b></p> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                                                                   | <p>(Optional) Exits to user EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Verifying that CE1 Can Communicate with CE2

Perform this task to verify that router CE1 has NLRI for router CE2.

## SUMMARY STEPS

- enable**
- show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]
- disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                        |
| Step 2 | <b>show ip route</b> [ <i>ip-address</i> [ <i>mask</i> ]<br>[ <b>longer-prefixes</b> ]]   [ <i>protocol</i> [ <i>process-id</i> ]]  <br>[ <b>list</b> <i>access-list-number</i>   <i>access-list-name</i> ]<br><br><b>Example:</b><br>Router# show ip route nn.nn.nn.nn<br><br><b>Example:</b><br>Router# show ip route | Displays the current state of the routing table. <ul style="list-style-type: none"> <li>Use the <i>ip-address</i> argument to verify that CE1 has a route to CE2.</li> <li>Use this command to verify the routes learned by CE1. Make sure that the route for CE2 is listed.</li> </ul> |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                                                                                | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                               |

## Verifying that PE1 Can Communicate with CE2

Perform this task to verify that router PE1 has NLRI for router CE2.

## SUMMARY STEPS

- enable
- show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list number** [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]] [**traffic-engineering** [*output-modifiers*]]
- show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [*ip-prefix/length*] [**longer-prefixes**] [*output-modifiers*] [*network-address* [*mask*] [**longer-prefixes**] [*output-modifiers*]] [**cidr-only**] [*community*] [**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**tags**]
- show ip cef [*vrf vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
- show mpls forwarding-table [{*network* {*mask* | *length*} | **labels** *label* [-*label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
- show ip bgp [*network*] [*network-mask*] [**longer-prefixes**]
- show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**summary**] [**labels**]
- disable

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                 |
| Step 2 | <p><b>show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]] [list number [output-modifiers]] [profile] [static [output-modifiers]] [summary [output-modifiers]] [supernets-only [output-modifiers]] [traffic-engineering [output-modifiers]]</b></p> <p><b>Example:</b><br/>Router# show ip route vrf vpn1 nn.nn.nn.nn</p>                                                                                                                                                                                     | <p>(Optional) Displays the IP routing table associated with a VRF.</p> <ul style="list-style-type: none"> <li>Use this command to verify that router PE1 learns routes from router CE2 (nn.nn.nn.nn).</li> </ul>                                        |
| Step 3 | <p><b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [ip-prefix/length] [longer-prefixes] [output-modifiers] [network-address [mask] [longer-prefixes] [output-modifiers]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [tags]</b></p> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 vrf vpn1 nn.nn.nn.nn</p> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 all nn.nn.nn.nn</p> | <p>(Optional) Displays VPN address information from the BGP table.</p> <ul style="list-style-type: none"> <li>Use the <b>vrf</b> or <b>all</b> keyword to verify that router PE2 is the BGP next-hop to router CE2.</li> </ul>                          |
| Step 4 | <p><b>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</b></p> <p><b>Example:</b><br/>Router# show ip cef vrf vpn1 nn.nn.nn.nn</p>                                                                                                                                                                                                                                                                                                                                                                                        | <p>(Optional) Displays entries in the forwarding information base (FIB) or displays a summary of the FIB.</p> <ul style="list-style-type: none"> <li>Use this command to verify that the Cisco Express Forwarding (CEF) entries are correct.</li> </ul> |
| Step 5 | <p><b>show mpls forwarding-table [{network {mask   length}   labels label [-label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]]] [detail]</b></p> <p><b>Example:</b><br/>Router# show mpls forwarding-table</p>                                                                                                                                                                                                                                                                                                           | <p>(Optional) Displays the contents of the MPLS LFIB.</p> <ul style="list-style-type: none"> <li>Use this command to verify the IGP label for the BGP next hop router (AS boundary).</li> </ul>                                                         |
| Step 6 | <p><b>show ip bgp [network] [network-mask] [longer-prefixes]</b></p> <p><b>Example:</b><br/>Router# show ip bgp ff.ff.ff.ff</p>                                                                                                                                                                                                                                                                                                                                                                                                                 | <p>(Optional) Displays entries in the BGP routing table.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip bgp</b> command to verify the label for the remote egress PE router (PE2).</li> </ul>                                            |

|        | Command or Action                                                                                                                                             | Purpose                                                                                                                                                                                                                |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <pre>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</pre> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 all labels</p> | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>summary</b> keywords to verify the VPN label of CE2, as advertised by PE2.</li> </ul> |
| Step 8 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                                 | (Optional) Exits to user EXEC mode.                                                                                                                                                                                    |

## Verifying that PE2 Can Communicate with CE2

Perform this task to ensure that PE2 can access CE2.

### SUMMARY STEPS

- enable
- show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]] [list number [output-modifiers]] [profile] [static [output-modifiers]] [summary [output-modifiers]] [supernets-only [output-modifiers]] [traffic-engineering [output-modifiers]]
- show mpls forwarding-table [vrf vrf-name] [{network {mask | length} | labels label [-label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]]] [detail]
- show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [summary] [labels]
- show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]
- disable

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                    |
| Step 2 | <pre>show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]] [list number [output-modifiers]] [profile] [static [output-modifiers]] [summary [output-modifiers]] [supernets-only [output-modifiers]] [traffic-engineering [output-modifiers]]</pre> <p><b>Example:</b><br/>Router# show ip route vrf vpn1 nn.nn.nn.nn</p> | (Optional) Displays the IP routing table associated with a VRF. <ul style="list-style-type: none"> <li>Use this command to check the VPN routing and forwarding table for CE2. The output provides next-hop information.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                         |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>show mpls forwarding-table [vrf vrf-name] [<i>{network {mask   length}   labels label</i> [<i>-label</i>]   interface interface   next-hop address   lsp-tunnel [tunnel-id]}] [detail]</pre> <p><b>Example:</b><br/>Router# show mpls forwarding-table vrf vpn1<br/>nn.nn.nn.nn</p> | <p>(Optional) Displays the contents of the LFIB.</p> <ul style="list-style-type: none"> <li>Use the <b>vrf</b> keyword to check the VPN routing and forwarding table for CE2. The output provides the label for CE2 and the outgoing interface.</li> </ul>      |
| Step 4 | <pre>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</pre> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 all labels</p>                                                                                                                            | <p>(Optional) Displays VPN address information from the BGP table.</p> <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>labels</b> keywords to check the VPN label for CE2 in the multiprotocol BGP table.</li> </ul>                           |
| Step 5 | <pre>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</pre> <p><b>Example:</b><br/>Router# show ip cef vpn1 nn.nn.nn.nn</p>                                                                                                                                        | <p>(Optional) Displays entries in the FIB or displays a summary of the FIB.</p> <ul style="list-style-type: none"> <li>Use this command to check the CEF entry for CE2. The command output shows the local label for CE2 and the outgoing interface.</li> </ul> |
| Step 6 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                                                                            | <p>(Optional) Exits to user EXEC mode.</p>                                                                                                                                                                                                                      |

## Verifying the ASBR Configuration

Perform this task to verify that the ASBRs exchange IPv4 routes with MPLS labels or IPv4 routes without labels as prescribed by a route map.

### SUMMARY STEPS

- enable
- show ip bgp [network] [network-mask] [longer-prefixes]
- show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]
- disable

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                          | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <p><b>show ip bgp</b> [<i>network</i>] [<i>network-mask</i>]<br/>[<i>longer-prefixes</i>]</p> <p><b>Example:</b><br/>Router# show ip bgp ff.ff.ff.ff</p> <p><b>Example:</b><br/>Router# show ip bgp bb.bb.bb.bb</p>                        | <p>(Optional) Displays entries in the BGP routing table.</p> <ul style="list-style-type: none"> <li>• Use this command to check that <ul style="list-style-type: none"> <li>– ASBR1 receives an MPLS label for PE2 from ASBR2.</li> <li>– ASBR1 receives IPv4 routes for RR2 without labels from ASBR2.</li> <li>– ASBR2 distributes an MPLS label for PE2 to ASBR1.</li> <li>– ASBR2 does not distribute a label for RR2 to ASBR1.</li> </ul> </li> </ul> |
| Step 3 | <p><b>show ip cef</b> [<i>vrf vrf-name</i>] [<i>network [mask]</i>]<br/>[<i>longer-prefixes</i>] [<i>detail</i>]</p> <p><b>Example:</b><br/>Router# show ip cef ff.ff.ff.ff</p> <p><b>Example:</b><br/>Router# show ip cef bb.bb.bb.bb</p> | <p>(Optional) Displays entries in the FIB or displays a summary of the FIB.</p> <ul style="list-style-type: none"> <li>• Use this command from ASBR1 and ASBR2 to check that <ul style="list-style-type: none"> <li>– The CEF entry for PE2 is correct.</li> <li>– The CEF entry for RR2 is correct.</li> </ul> </li> </ul>                                                                                                                                |
| Step 4 | <p><b>disable</b></p> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                           | <p>(Optional) Exits to user EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                 |

# Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

Configuration examples for MPLS VPN Inter-AS include the following:

- [Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over an MPLS VPN Service Provider: Examples, page 20](#)
- [Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over a Non MPLS VPN Service Provider: Examples, page 25](#)

## Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over an MPLS VPN Service Provider: Examples

Configuration examples for Inter-AS using BGP to distribute routes and MPLS labels over an MPLS VPN service provider included in this section are as follows:

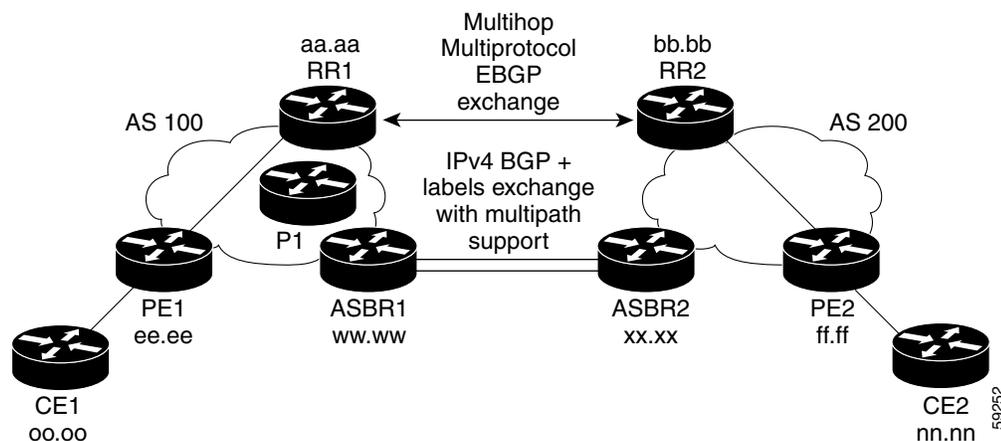
- [Route Reflector 1 Configuration Example \(MPLS VPN Service Provider\), page 21](#)
- [ASBR1 Configuration Example \(MPLS VPN Service Provider\), page 22](#)
- [Route Reflector 2 Configuration Example \(MPLS VPN Service Provider\), page 23](#)
- [ASBR2 Configuration Example \(MPLS VPN Service Provider\), page 24](#)

Figure 4 shows two MPLS VPN service providers. The service provider distributes the VPN-IPv4 routes between the route reflectors. The MPLS VPN SPs distribute the IPv4 routes with MPLS labels between the ASBRs.

The configuration example shows the two techniques you can use to distribute the VPN-IPv4 routes and the IPv4 routes with MPLS labels of the remote RRs and PEs to the local RRs and PEs:

- AS 100 uses the RRs to distribute the VPN-IPv4 routes learned from the remote RRs. The RRs also distribute the remote PE address and label learned from ASBR1 using IPv4 + labels.
- In AS 200, the IPv4 routes that ASBR2 learned are redistributed into IGP.

**Figure 4** *Distributing IPv4 Routes and MPLS Labels Between MPLS VPN Service Providers*



## Route Reflector 1 Configuration Example (MPLS VPN Service Provider)

The configuration example for RR1 specifies the following:

- RR1 exchanges VPN-IPv4 routes with RR2 using multiprotocol, multihop eBGP.
- The VPN-IPv4 next-hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1:
  - The VPN-IPv4 routes learned from RR2
  - The IPv4 routes and MPLS labels learned from ASBR1

```

ip subnet-zero
ip cef
!
interface Loopback0
 ip address aa.aa.aa.aa 255.255.255.255
!
interface Ethernet0/3
 ip address dd.0.0.2 255.0.0.0
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network aa.aa.aa.aa 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor ee.aa.aa.aa remote-as 100
 neighbor ee.aa.aa.aa update-source Loopback0
 neighbor ww.ww.ww.ww remote-as 100
 neighbor ww.ww.ww.ww update-source Loopback0
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb ebgp-multihop 255
 neighbor bb.bb.bb.bb update-source Loopback0
 no auto-summary
!
address-family ipv4
 neighbor ee.aa.aa.aa activate
 neighbor ee.aa.aa.aa route-reflector-client !IPv4+labels session to PE1
 neighbor ee.aa.aa.aa send-label
 neighbor ww.ww.ww.ww activate
 neighbor ww.ww.ww.ww route-reflector-client !IPv4+labels session to ASBR1
 neighbor ww.ww.ww.ww send-label
 no neighbor bb.bb.bb.bb activate
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpnv4
 neighbor ee.aa.aa.aa activate
 neighbor ee.aa.aa.aa route-reflector-client !VPNv4 session with PE1
 neighbor ee.aa.aa.aa send-community extended
 neighbor bb.bb.bb.bb activate
 neighbor bb.bb.bb.bb next-hop-unchanged !MH-VPNv4 session with RR2
 neighbor bb.bb.bb.bb send-community extended !with next hop unchanged
 exit-address-family
!
ip default-gateway 3.3.0.1

```

```

no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end

```

## ASBR1 Configuration Example (MPLS VPN Service Provider)

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

In this example, ASBR1 uses route maps to filter routes.

- A route map called OUT specifies that ASBR1 should distribute the PE1 route (ee.ee) with labels and the RR1 route (aa.aa) without labels.
- A route map called IN specifies that ASBR1 should accept the PE2 route (ff.ff) with labels and the RR2 route (bb.bb) without labels.

```

ip subnet-zero
mpls label protocol ldp
!
interface Loopback0
 ip address ww.ww.ww.ww 255.255.255.255
!
interface Ethernet0/2
 ip address hh.0.0.2 255.0.0.0
!
interface Ethernet0/3
 ip address dd.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network ww.ww.ww.ww 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100

router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor hh.0.0.1 remote-as 200
 no auto-summary
!
!
address-family ipv4
 redistribute ospf 10
 neighbor aa.aa.aa.aa activate
 neighbor aa.aa.aa.aa send-label
 neighbor hh.0.0.1 activate
 neighbor hh.0.0.1 advertisement-interval 5
 neighbor hh.0.0.1 send-label
 neighbor hh.0.0.1 route-map IN in
 neighbor hh.0.0.1 route-map OUT out

```

! Redistributing IGP into BGP  
! so that PE1 & RR1 loopbacks  
! get into the BGP table  
  
! accepting routes in route map IN.  
! distributing routes in route map OUT.

```

neighbor kk.0.0.1 activate
neighbor kk.0.0.1 advertisement-interval 5
neighbor kk.0.0.1 send-label
neighbor kk.0.0.1 route-map IN in ! accepting routes in route map IN.
neighbor kk.0.0.1 route-map OUT out ! distributing routes in route map OUT.
no auto-summary
no synchronization
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ee.ee.ee.ee log !Setting up the access lists
access-list 2 permit ff.ff.ff.ff log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log

route-map IN permit 10 !Setting up the route maps
 match ip address 2
 match mpls-label
!
route-map IN permit 11
 match ip address 4
!
route-map OUT permit 12
 match ip address 3
!
route-map OUT permit 13
 match ip address 1
 set mpls-label
!
end

```

## Route Reflector 2 Configuration Example (MPLS VPN Service Provider)

RR2 exchanges VPN-IPv4 routes with RR1 through multihop, multiprotocol eBGP. This configuration also specifies that the next hop information and the VPN label are preserved across the autonomous systems.

```

ip subnet-zero
ip cef
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
 ip address ii.0.0.2 255.0.0.0
!
router ospf 20
 log-adjacency-changes
 network bb.bb.bb.bb 0.0.0.0 area 200
 network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa ebgp-multihop 255
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor ff.ff.ff.ff remote-as 200
 neighbor ff.ff.ff.ff update-source Loopback0

```

```

no auto-summary
!
address-family vpnv4
neighbor aa.aa.aa.aa activate
neighbor aa.aa.aa.aa next-hop-unchanged !Multihop VPNv4 session with RR1
neighbor aa.aa.aa.aa send-community extended !with next-hop-unchanged
neighbor ff.ff.ff.ff activate
neighbor ff.ff.ff.ff route-reflector-client !VPNv4 session with PE2
neighbor ff.ff.ff.ff send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
end

```

## ASBR2 Configuration Example (MPLS VPN Service Provider)

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can now reach these prefixes.

```

ip subnet-zero
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet1/0
 ip address hh.0.0.1 255.0.0.0
!
interface Ethernet1/2
 ip address jj.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 20
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 200 subnets ! Redistributing the routes learned from
 passive-interface Ethernet1/0 ! ASBR1(eBGP+labels session) into IGP
 network xx.xx.xx.xx 0.0.0.0 area 200 ! so that PE2 will learn them
 network jj..0.0 0.255.255.255 area 200
!
router bgp 200
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb update-source Loopback0
 neighbor hh.0.0.2 remote-as 100
 no auto-summary
!
address-family ipv4
 redistribute ospf 20 ! Redistributing IGP into BGP
 neighbor hh.0.0.2 activate ! so that PE2 & RR2 loopbacks
 neighbor hh.0.0.2 advertisement-interval 5 ! will get into the BGP-4 table.
 neighbor hh.0.0.2 route-map IN in
 neighbor hh.0.0.2 route-map OUT out
 neighbor hh.0.0.2 send-label

```

```
neighbor kk.0.0.2 activate
neighbor kk.0.0.2 advertisement-interval 5
neighbor kk.0.0.2 route-map IN in
neighbor kk.0.0.2 route-map OUT out
neighbor kk.0.0.2 send-label
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor bb.bb.bb.bb activate
neighbor bb.bb.bb.bb send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ff.ff.ff.ff log !Setting up the access lists
access-list 2 permit ee.ee.ee.ee log
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log

route-map IN permit 11 !Setting up the route maps
match ip address 2
match mpls-label
!
route-map IN permit 12
match ip address 4
!
route-map OUT permit 10
match ip address 1
set mpls-label
!
route-map OUT permit 13
match ip address 3
end
```

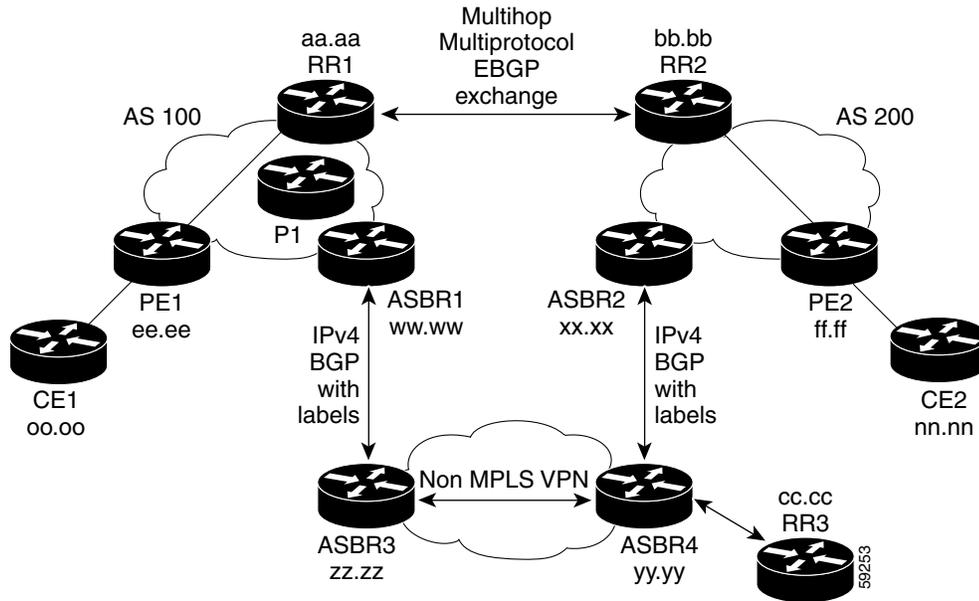
## Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over a Non MPLS VPN Service Provider: Examples

Configuration examples for Inter-AS using BGP to distribute routes and MPLS labels over a non MPLS VPN service provider included in this section are as follows:

- [Route Reflector 1 Configuration Example \(Non MPLS VPN Service Provider\), page 27](#)
- [ASBR1 Configuration Example \(Non MPLS VPN Service Provider\), page 28](#)
- [Route Reflector 2 Configuration Example \(Non MPLS VPN Service Provider\), page 29](#)
- [ASBR2 Configuration Example \(Non MPLS VPN Service Provider\), page 30](#)
- [ASBR3 Configuration Example \(Non MPLS VPN Service Provider\), page 31](#)
- [Route Reflector 3 Configuration Example \(Non MPLS VPN Service Provider\), page 33](#)
- [ASBR4 Configuration Example \(Non MPLS VPN Service Provider\), page 34](#)

Figure 5 shows two MPLS VPN service providers that are connected through a non MPLS VPN service provider. The autonomous system in the middle of the network is configured as a backbone autonomous system that uses Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP) to distribute MPLS labels. You can also use traffic engineering tunnels instead of TDP or LDP to build the LSP across the non MPLS VPN service provider.

**Figure 5** *Distributing Routes and MPLS Labels Over a Non MPLS VPN Service Provider*



## Route Reflector 1 Configuration Example (Non MPLS VPN Service Provider)

The configuration example for RR1 specifies the following:

- RR1 exchanges VPN-IPv4 routes with RR2 using multiprotocol, multihop eBGP.
- The VPN-IPv4 next-hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1:
  - The VPN-IPv4 routes learned from RR2
  - The IPv4 routes and MPLS labels learned from ASBR1

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address aa.aa.aa.aa 255.255.255.255
!
interface Serial1/2
 ip address dd.0.0.2 255.0.0.0
 clockrate 124061
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network aa.aa.aa.aa 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor ee.aa.aa.aa remote-as 100
 neighbor ee.aa.aa.aa update-source Loopback0
 neighbor ww.ww.ww.ww remote-as 100
 neighbor ww.ww.ww.ww update-source Loopback0
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb ebgp-multihop 255
 neighbor bb.bb.bb.bb update-source Loopback0
 no auto-summary
!
address-family ipv4
 neighbor ee.aa.aa.aa activate
 neighbor ee.aa.aa.aa route-reflector-client !IPv4+labels session to PE1
 neighbor ee.aa.aa.aa send-label
 neighbor ww.ww.ww.ww activate
 neighbor ww.ww.ww.ww route-reflector-client !IPv4+labels session to ASBR1
 neighbor ww.ww.ww.ww send-label
 no neighbor bb.bb.bb.bb activate
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpnv4
 neighbor ee.aa.aa.aa activate
 neighbor ee.aa.aa.aa route-reflector-client !VPNv4 session with PE1
 neighbor ee.aa.aa.aa send-community extended
 neighbor bb.bb.bb.bb activate
 neighbor bb.bb.bb.bb next-hop-unchanged !MH-VPNv4 session with RR2
 neighbor bb.bb.bb.bb send-community extended with next-hop-unchanged
 exit-address-family
!
```

```

ip default-gateway 3.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end

```

## ASBR1 Configuration Example (Non MPLS VPN Service Provider)

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

In this example, ASBR1 uses route maps to filter routes.

- A route map called OUT specifies that ASBR1 should distribute the PE1 route (ee.ee) with labels and the RR1 route (aa.aa) without labels.
- A route map called IN specifies that ASBR1 should accept the PE2 route (ff.ff) with labels and the RR2 route (bb.bb) without labels.

```

ip subnet-zero
ip cef distributed
mpls label protocol ldp
!
interface Loopback0
 ip address ww.ww.ww.ww 255.255.255.255
!
interface Serial3/0/0
 ip address kk.0.0.2 255.0.0.0
 ip route-cache distributed
!
interface Ethernet0/3
 ip address dd.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Serial3/0/0
 network ww.ww.ww.ww 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100

router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor kk.0.0.1 remote-as 200
 no auto-summary
!
 address-family ipv4
 redistribute ospf 10 ! Redistributing IGP into BGP
 neighbor aa.aa.aa.aa activate ! so that PE1 & RR1 loopbacks
 neighbor aa.aa.aa.aa send-label ! get into BGP table
 neighbor kk.0.0.1 activate
 neighbor kk.0.0.1 advertisement-interval 5
 neighbor kk.0.0.1 send-label
 neighbor kk.0.0.1 route-map IN in ! Accepting routes specified in route map IN

```

```

neighbor kk.0.0.1 route-map OUT out ! Distributing routes specified in route map OUT
no auto-summary
no synchronization
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ee.aa.aa.aa log
access-list 2 permit ff.aa.aa.aa log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log
!
route-map IN permit 10
 match ip address 2
 match mpls-label
!
route-map IN permit 11
 match ip address 4
!
route-map OUT permit 12
 match ip address 3
!
route-map OUT permit 13
 match ip address 1
 set mpls-label
!
end

```

## Route Reflector 2 Configuration Example (Non MPLS VPN Service Provider)

RR2 exchanges VPN-IPv4 routes with RR1 using multihop, multiprotocol eBGP. This configuration also specifies that the next hop information and the VPN label are preserved across the autonomous systems.

```

ip subnet-zero
ip cef
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
 ip address ii.0.0.2 255.0.0.0
!
router ospf 20
 log-adjacency-changes
 network bb.bb.bb.bb 0.0.0.0 area 200
 network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa ebgp-multihop 255
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor ff.ff.ff.ff remote-as 200
 neighbor ff.ff.ff.ff update-source Loopback0
 no auto-summary
!
address-family vpnv4
 neighbor aa.aa.aa.aa activate
 neighbor aa.aa.aa.aa next-hop-unchanged
!MH vpnv4 session with RR1

```

```

neighbor aa.aa.aa.aa send-community extended !with next-hop-unchanged
neighbor ff.ff.ff.ff activate
neighbor ff.ff.ff.ff route-reflector-client !vpngv4 session with PE2
neighbor ff.ff.ff.ff send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
end

```

## ASBR2 Configuration Example (Non MPLS VPN Service Provider)

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can now reach these prefixes.

```

ip subnet-zero
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet0/1
 ip address qq.0.0.2 255.0.0.0
!
interface Ethernet1/2
 ip address jj.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 20
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 200 subnets !redistributing the routes learned from
 passive-interface Ethernet0/1 !ASBR2 (eBGP+labels session) into IGP
 network xx.xx.xx.xx 0.0.0.0 area 200 !so that PE2 will learn them
 network jj.0.0.0 0.255.255.255 area 200
!
router bgp 200
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb update-source Loopback0
 neighbor qq.0.0.1 remote-as 100
 no auto-summary
!
address-family ipv4 ! Redistributing IGP into BGP
 redistribute ospf 20 ! so that PE2 & RR2 loopbacks
 neighbor qq.0.0.1 activate ! will get into the BGP-4 table
 neighbor qq.0.0.1 advertisement-interval 5
 neighbor qq.0.0.1 route-map IN in
 neighbor qq.0.0.1 route-map OUT out
 neighbor qq.0.0.1 send-label
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpngv4

```

```
neighbor bb.bb.bb.bb activate
neighbor bb.bb.bb.bb send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ff.ff.ff.ff log
access-list 2 permit ee.ee.ee.ee log
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log
!
route-map IN permit 11
 match ip address 2
 match mpls-label
!
route-map IN permit 12
 match ip address 4
!
route-map OUT permit 10
 match ip address 1
 set mpls-label
!
route-map OUT permit 13
 match ip address 3
!
end
```

## ASBR3 Configuration Example (Non MPLS VPN Service Provider)

ASBR3 belongs to a non MPLS VPN service provider. ASBR3 exchanges IPv4 routes and MPLS labels with ASBR1. ASBR3 also passes the routes learned from ASBR1 to ASBR3 through RR3.

**Note**

---

Do not redistribute eBGP routes learned into iBGP if you are using iBGP to distribute the routes and labels. This is not a supported configuration.

---

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address yy.yy.yy.yy 255.255.255.255
```

```

interface Hssi4/0
 ip address mm.0.0.0.1 255.0.0.0
 mpls ip
 hssi internal-clock
 !
interface Serial5/0
 ip address kk.0.0.1 255.0.0.0
 load-interval 30
 clockrate 124061
 !
router ospf 30
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 network yy.yy.yy.yy 0.0.0.0 area 300
 network mm.0.0.0 0.255.255.255 area 300
 !
router bgp 300
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor cc.cc.cc.cc remote-as 300
 neighbor cc.cc.cc.cc update-source Loopback0
 neighbor kk.0.0.2 remote-as 100
 no auto-summary
 !
 address-family ipv4
 neighbor cc.cc.cc.cc activate ! iBGP+labels session with RR3
 neighbor cc.cc.cc.cc send-label
 neighbor kk.0.0.2 activate ! eBGP+labels session with ASBR1
 neighbor kk.0.0.2 advertisement-interval 5
 neighbor kk.0.0.2 send-label
 neighbor kk.0.0.2 route-map IN in
 neighbor kk.0.0.2 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
 !
ip classless
 !
access-list 1 permit ee.aa.aa.aa log
access-list 2 permit ff.ff.ff.ff log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log
 !
route-map IN permit 10
 match ip address 1
 match mpls-label
 !
route-map IN permit 11
 match ip address 3
 !
route-map OUT permit 12
 match ip address 2
 set mpls-label
 !
route-map OUT permit 13
 match ip address 4
 !

```

```

ip default-gateway 3.3.0.1
ip classless
!
end

```

## Route Reflector 3 Configuration Example (Non MPLS VPN Service Provider)

RR3 is a non MPLS VPN RR that reflects IPv4 routes with MPLS labels to ASBR3 and ASBR4.

```

ip subnet-zero
mpls label protocol ldp
mpls traffic-eng auto-bw timers
no mpls ip
!
interface Loopback0
 ip address cc.cc.cc.cc 255.255.255.255
!
interface POS0/2
 ip address pp.0.0.1 255.0.0.0
 crc 16
 clock source internal
!
router ospf 30
 log-adjacency-changes
 network cc.cc.cc.cc 0.0.0.0 area 300
 network pp.0.0.0 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 neighbor zz.zz.zz.zz remote-as 300
 neighbor zz.zz.zz.zz update-source Loopback0
 neighbor yy.yy.yy.yy remote-as 300
 neighbor yy.yy.yy.yy update-source Loopback0
 no auto-summary
!
address-family ipv4
 neighbor zz.zz.zz.zz activate
 neighbor zz.zz.zz.zz route-reflector-client
 neighbor zz.zz.zz.zz send-label ! iBGP+labels session with ASBR3
 neighbor yy.yy.yy.yy activate
 neighbor yy.yy.yy.yy route-reflector-client
 neighbor yy.yy.yy.yy send-label ! iBGP+labels session with ASBR4
 no auto-summary
 no synchronization
 exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
end

```

## ASBR4 Configuration Example (Non MPLS VPN Service Provider)

ASBR4 belongs to a non MPLS VPN service provider. ASBR4 and ASBR3 exchange IPv4 routes and MPLS labels by means of RR3.



### Note

Do not redistribute eBGP routes learned into iBGP if you are using iBGP to distribute the routes and labels. This is not a supported configuration.

```

ip subnet-zero
ip cef distributed
!
interface Loopback0
 ip address zz.zz.zz.zz 255.255.255.255
!
interface Ethernet0/2
 ip address qq.0.0.1 255.0.0.0
!
interface POS1/1/0
 ip address pp.0.0.2 255.0.0.0
 ip route-cache distributed
!
interface Hssi2/1/1
 ip address mm.0.0.2 255.0.0.0
 ip route-cache distributed
 mpls label protocol ldp
 mpls ip
 hssi internal-clock
!
router ospf 30
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network zz.zz.zz.zz 0.0.0.0 area 300
 network pp.0.0.0 0.255.255.255 area 300
 network mm.0.0.0 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor cc.cc.cc.cc remote-as 300
 neighbor cc.cc.cc.cc update-source Loopback0
 neighbor qq.0.0.2 remote-as 200
 no auto-summary
!
 address-family ipv4
 neighbor cc.cc.cc.cc activate
 neighbor cc.cc.cc.cc send-label
 neighbor qq.0.0.2 activate
 neighbor qq.0.0.2 advertisement-interval 5
 neighbor qq.0.0.2 send-label
 neighbor qq.0.0.2 route-map IN in
 neighbor qq.0.0.2 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
!
access-list 1 permit ff.ff.ff.ff log
access-list 2 permit ee.ee.ee.ee log

```

```
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log
!
route-map IN permit 10
 match ip address 1
 match mpls-label
!
route-map IN permit 11
 match ip address 3
!
route-map OUT permit 12
 match ip address 2
 set mpls-label
!
route-map OUT permit 13
 match ip address 4
!
ip default-gateway 3.3.0.1
ip classless
!
end
```

## Additional References

The following sections provide references related to MPLS VPNs.

### Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC      | Title                                                  |
|----------|--------------------------------------------------------|
| RFC 1700 | <i>Assigned Numbers</i>                                |
| RFC 1966 | BGP Route Reflection: An Alternative to Full Mesh IBGP |
| RFC 2842 | Capabilities Advertisement with BGP-4                  |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>              |
| RFC 3107 | <i>Carrying Label Information in BGP-4</i>             |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

Table 2 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

| Feature Name                                                    | Releases                                                                                              | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN Inter-Autonomous Systems - IPv4 BGP Label Distribution | 12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.0(24)S<br>12.2(14)S<br>12.0(27)S<br>12.0(29)S | <p>This module explains how to configure an MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPN-IPv4 routes by using multihop, multiprotocol, External Border Gateway Protocol (eBGP).</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Information About Using MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 4</a></li> <li><a href="#">How to Configure MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 6</a></li> </ul> |

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS VPN Carrier Supporting Carrier Using LDP and an IGP

---

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Carrier Supporting Carrier (CSC) enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. This module explains how to configure the MPLS VPN CSC network using MPLS Label Distribution Protocol (LDP) to distribute MPLS labels and an Interior Gateway Protocol (IGP) to distribute routes.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for MPLS VPN CSC with LDP and IGP”](#) section on page 65.

## Contents

- [Prerequisites for MPLS VPN CSC with LDP and IGP, page 1](#)
- [Restrictions for MPLS VPN CSC with LDP and IGP, page 2](#)
- [Information About MPLS VPN CSC with LDP and IGP, page 3](#)
- [How to Configure MPLS VPN CSC with LDP and IGP, page 9](#)
- [Configuration Examples for MPLS VPN CSC with LDP and IGP, page 18](#)
- [Additional References, page 65](#)
- [Feature Information for MPLS VPN CSC with LDP and IGP, page 65](#)

## Prerequisites for MPLS VPN CSC with LDP and IGP

This feature includes the following requirements:

- The provider edge (PE) routers of the backbone carrier require 128 MB of memory.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- The backbone carrier must enable the PE router to check that the packets it receives from the customer edge (CE) router contain only the labels that the PE router advertised to the CE router. This prevents data spoofing, which occurs when a packet from an unrecognized IP address is sent to a router.

## Restrictions for MPLS VPN CSC with LDP and IGP

The following features are not supported with this feature:

- ATM MPLS
- Carrier supporting carrier traffic engineering
- Carrier supporting carrier quality of service (QoS)
- RSVP aggregation
- VPN Multicast between the customer carrier and the backbone carrier network

The following router platforms are supported on the edge of the MPLS VPN:

- Cisco 7200 series
- Cisco 7500 series
- Cisco 12000 series

See [Table 1](#) for Cisco 12000 series line card support added for Cisco IOS releases.

**Table 1** Cisco 12000 Series Line Card Support Added for Cisco IOS Releases

| Type                             | Line Cards            | Cisco IOS Release Added |
|----------------------------------|-----------------------|-------------------------|
| Packet Over SONET (POS)          | 4-Port OC-3 POS       | 12.0(16)ST              |
|                                  | 1-Port OC-12 POS      |                         |
|                                  | 8-Port OC-3 POS       | 12.0(21)ST              |
|                                  | 16-Port OC-3 POS      |                         |
|                                  | 4-Port OC-12 POS      |                         |
|                                  | 1-Port OC-48 POS      |                         |
|                                  | 4-Port OC-3 POS ISE   | 12.0(22)S               |
|                                  | 8-Port OC-3 POS ISE   |                         |
|                                  | 16 x OC-3 POS ISE     |                         |
|                                  | 4 Port OC-12 POS ISE  |                         |
| 1-Port OC-48 POS ISE             |                       |                         |
| Electrical Interface             | 6- Port DS3           | 12.0(16)ST              |
|                                  | 12- Port DS3          |                         |
|                                  | 6-Port E3             | 12.0(21)ST              |
| Asynchronous Transfer Mode (ATM) | 4-Port OC-3 ATM       | 12.0(22)S               |
|                                  | 1-Port OC12 ATM       |                         |
|                                  | 4-Port OC-12 ATM      |                         |
| Channelized Interface            | 2-Port CHOC-3         | 12.0(22)S               |
|                                  | 6-Port Ch T3 (DS1)    |                         |
|                                  | 1-Port CHOC-12 (DS3)  |                         |
|                                  | 1-Port CHOC-12 (OC-3) |                         |
|                                  | 4-Port CHOC-12 ISE    |                         |
| 1-Port CHOC-48 ISE               |                       |                         |

# Information About MPLS VPN CSC with LDP and IGP

Before configuring MPLS VPN CSC, you should understand the following concepts:

- [MPLS VPN CSC Introduction, page 3](#)
- [Benefits of Implementing MPLS VPN CSC, page 3](#)
- [Configuration Options for MPLS VPN CSC with LDP and IGP, page 4](#)

## MPLS VPN CSC Introduction

Carrier supporting carrier is a term used to describe a situation where one service provider allows another service provider 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.

A backbone carrier offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services. The customer carrier can be either:

- An Internet service provider (ISP)
- A BGP/MPLS VPN service provider

This document uses the following terminology:

- *CE router*: A customer edge router is part of a customer network and interfaces to a provider edge (PE) router. In this document, the CE router sits on the edge of the customer carrier network.
- *PE router*: A provider edge router is part of a service provider's network connected to a customer CE router. In this document, the PE routers sit on the edge of the backbone carrier network.
- *ASBR*: An autonomous system boundary router connects one autonomous system to another.

## Benefits of Implementing MPLS VPN CSC

The MPLS VPN CSC provides the following benefits to service providers who are backbone carriers and to customer carriers.

### Benefits to the Backbone Carrier

- The backbone carrier can accommodate many customer carriers and give them access to its backbone. The backbone carrier does not need to create and maintain separate backbones for its customer carriers. Using one backbone network to support multiple customer carriers simplifies the backbone carrier's VPN operations. The backbone carrier uses a consistent method for managing and maintaining the backbone network. This is also cheaper and more efficient than maintaining separate backbones.
- The MPLS VPN carrier supporting carrier feature is scalable. Carrier supporting carrier can change the VPN to meet changing bandwidth and connectivity needs. The feature can accommodate unplanned growth and changes. The carrier supporting carrier feature enables tens of thousands of VPNs to be set up over the same network, and it allows a service provider to offer both VPN and Internet services.
- The MPLS VPN carrier supporting carrier feature is a flexible solution. The backbone carrier can accommodate many types of customer carriers. The backbone carrier can accept customer carriers who are ISPs or VPN service providers or both. The backbone carrier can accommodate customer carriers that require security and various bandwidths.

### Benefits to the Customer Carriers

- The MPLS VPN carrier supporting carrier feature removes from the customer carrier the burden of configuring, operating, and maintaining its own backbone. The customer carrier uses the backbone network of a backbone carrier, but the backbone carrier is responsible for network maintenance and operation.
- Customer carriers who use the VPN services provided by the backbone carrier receive the same level of security that Frame Relay or ATM-based VPNs provide. Customer carriers can also use IPSec in their VPNs for a higher level of security; it is completely transparent to the backbone carrier.
- Customer carriers can use any link layer technology (SONET, DSL, Frame Relay, and so on) to connect the CE routers to the PE routers and the PE routers to the P routers. The MPLS VPN carrier supporting carrier feature is link layer independent. The CE routers and PE routers use IP to communicate, and the backbone carrier uses MPLS.
- The customer carrier can use any addressing scheme and still be supported by a backbone carrier. The customer address space and routing information are independent of the address space and routing information of other customer carriers or the backbone provider.

## Configuration Options for MPLS VPN CSC with LDP and IGP

The backbone carrier offers BGP and MPLS VPN services. The customer carrier can be either of the following:

- [Customer Carrier Is an ISP, page 4](#)
- [Customer Carrier Is a BGP/MPLS VPN Service Provider, page 7](#)

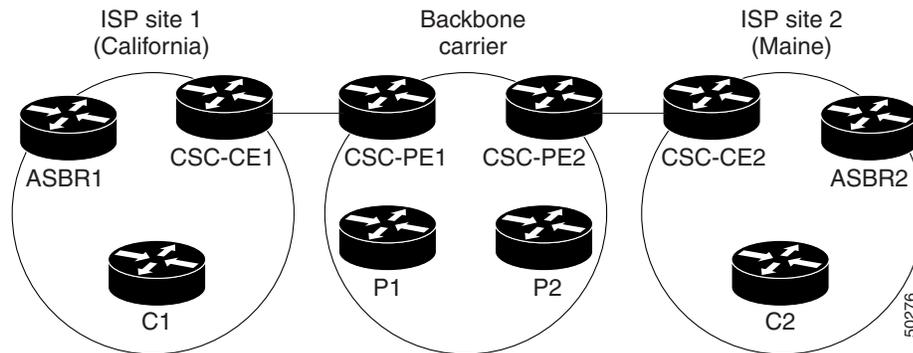
The following sections explain how the backbone and customer carriers distribute IPv4 routes and MPLS labels.

### Customer Carrier Is an ISP

This section explains how a BGP/MPLS VPN service provider (backbone carrier) can provide a segment of its backbone network to a customer who is an ISP.

Consider the following example:

An ISP has two sites: one in California, the other in Maine. Each site is a point of presence (POP). The ISP wants to connect these sites using a VPN service provided by a backbone carrier. [Figure 1](#) illustrates this situation.

**Figure 1** Sample BGP/MPLS Backbone Carrier Supporting an ISP**Note**

The CE routers in the figures in this module are CE routers to the backbone carrier. However, they are PE routers to the 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 CE routers of the customer carrier and the PE routers of the backbone carrier.
- MPLS is enabled on the interface between the CE router of the customer carrier and the PE router of the backbone carrier.

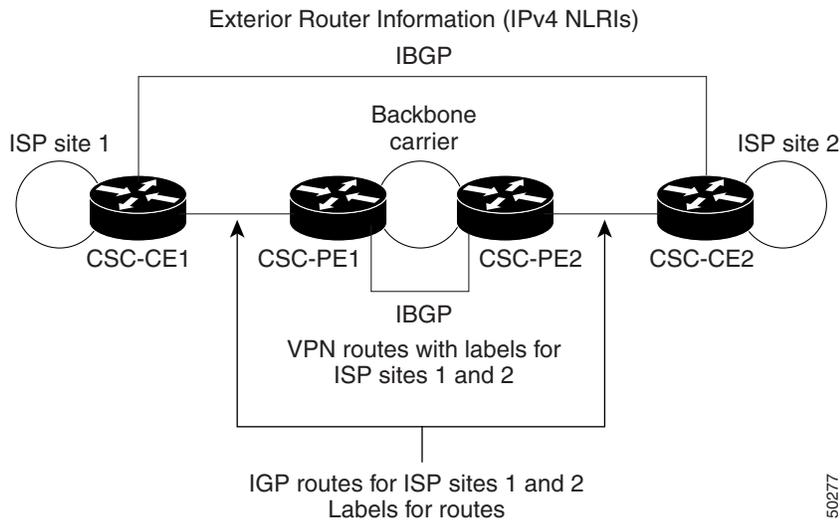
Internal and external routes are differentiated this way:

- 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 CE routers of the customer carrier and the PE routers of the backbone carrier significantly reduces the number of routes that the PE router needs to maintain.

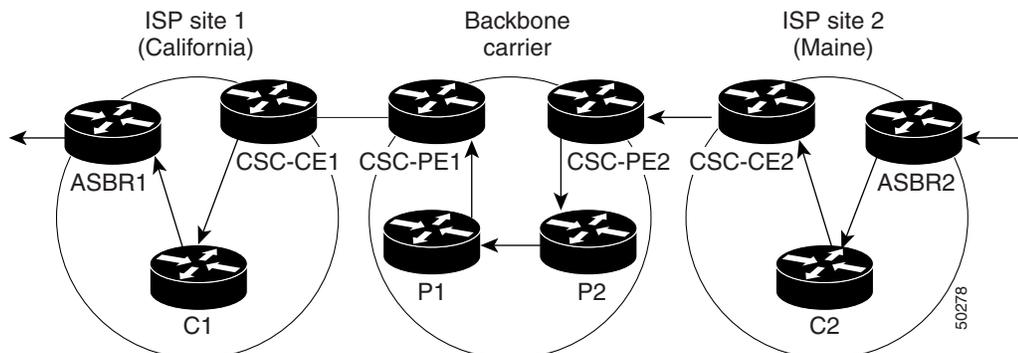
Since the PE routers do not have to carry external routes in the VRF routing table, they can use the incoming label in the packet to forward the customer carrier Internet traffic. Adding MPLS to the routers provides a consistent method of transporting packets from the customer carrier to the backbone carrier. MPLS allows the exchange of an MPLS label between the PE and the 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 2](#) shows how information is exchanged when the network is configured in this manner.

**Figure 2** Backbone Carrier Exchanging Routing Information with a Customer Carrier Who Is an ISP



In [Figure 3](#), routes are created between the backbone carrier and the customer carrier sites. ASBR2 receives an Internet route that originated outside the network. All routers in the ISP sites have all the external routes through IBGP connections among them.

**Figure 3** Establishing a Route Between a Backbone Carrier and a Customer Carrier Who Is an ISP



[Table 2](#) describes the process of establishing the route, which can be divided into two distinct steps:

- The backbone carrier propagates the IGP information of the customer carrier, which enables the customer carrier routers to reach all the customer carrier routers in the remote sites.
- Once the routers of the customer carriers in different sites are reachable, external routes can be propagated in the customer carrier sites, using IBGP without using the backbone carrier routers.

**Table 2**      **Establishing a Route Between the Backbone Carrier and the Customer Carrier ISP**

| Step | Description                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | CSC-CE2 sends the internal routes within site 2 to CSC-PE2. The routes include the route to ASBR2.                                                                                                                                                                                    |
| 2    | CSC-PE2 sends the routing information for site 2 to CSC-PE1, using MPLS VPN processes. CSC-PE1 gets one label (called L3), which is associated with the route to the VPN-IP address for ASBR2. CSC-PE1 gets another label (called L2), which is associated with the route to CSC-PE2. |
| 3    | CSC-PE1 sends the routing information associated with internal routes from site 2 to CSC-CE1. CSC-PE1 also sends the label binding information. As a result, CSC-CE1 gets the route to ASBR2 with CSC-PE1 as the next hop. The label associated with that route is called L1.         |
| 4    | CSC-CE1 distributes the routing information through site 1. Every router in site 1 gets a route for every internal destination in site 2. Therefore, every router in site 1 can reach routers in site 2 and learn external routes through IBGP.                                       |
| 5    | ASBR2 receives an Internet route.                                                                                                                                                                                                                                                     |
| 6    | The IBGP sessions exchange the external routing information of the ISP, including a route to the Internet. Every router in site 1 knows a route to the Internet, with ASBR2 as the next hop of that route.                                                                            |

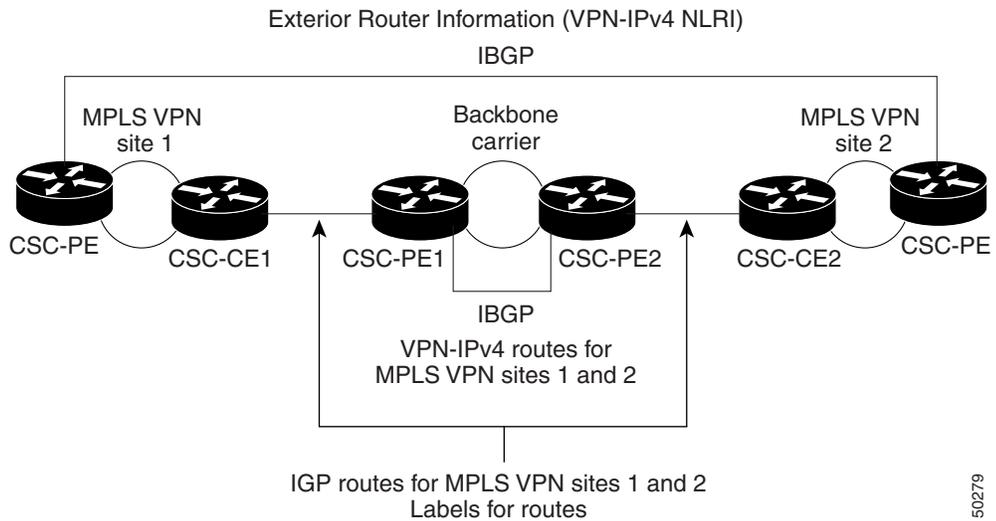
## Customer Carrier Is a BGP/MPLS VPN Service Provider

When a backbone carrier and the customer carrier both provide BGP/MPLS VPN services, the method of transporting data is different from when a customer carrier provides only ISP services. The following list highlights those differences:

- When a customer carrier provides BGP/MPLS VPN services, its external routes are VPN-IPv4 routes. When a customer carrier is an ISP, its external routes are IP routes.
- When a customer carrier provides BGP/MPLS VPN services, every site within the customer carrier must use MPLS. When a customer carrier is an ISP, the sites do not need to use MPLS.

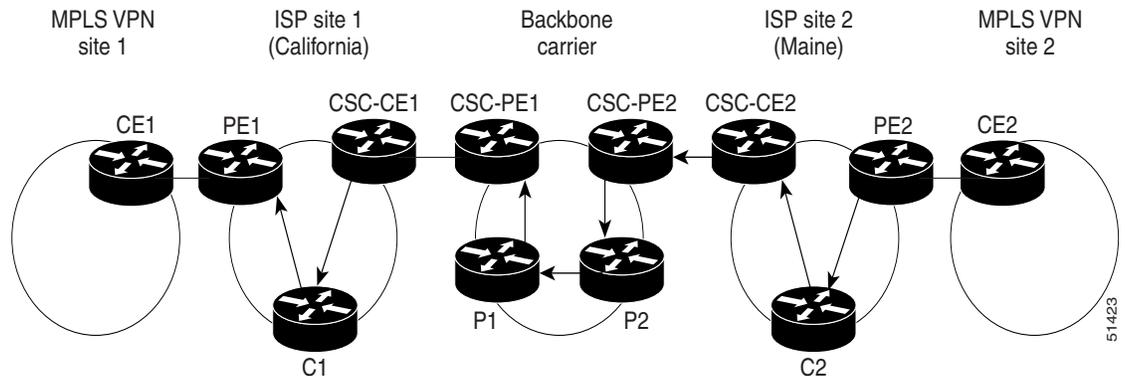
Figure 4 shows how information is exchanged when MPLS VPN services reside on all customer carrier sites and on the backbone carrier.

**Figure 4** Backbone Carrier Exchanging Information with a Customer Carrier Who Is an MPLS VPN Service Provider



In the example shown in [Figure 5](#), routes are created between the backbone carrier and the customer carrier sites.

**Figure 5** Establishing a Route Between a Backbone Carrier and a Customer Carrier Who Is an MPLS VPN Service Provider



[Table 3](#) describes the process of establishing the route.

**Table 3** Establishing a Route Between the Backbone Carrier and Customer Carrier Site

| Step | Description                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | CE2 sends all the internal routes within site 2 to CSC-PE2.                                                                                                                                                                                                                         |
| 2    | CSC-PE2 sends the routing information for site 2 to CSC-PE1, using MPLS VPN processes. CSC-PE1 gets one label (called L3), which is associated with the route to the VPN-IP address for PE2. CSC-PE1 gets another label (called L2), which is associated with the route to CSC-PE2. |

**Table 3**      **Establishing a Route Between the Backbone Carrier and Customer Carrier Site**

| Step | Description                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3    | CSC-PE1 sends the routing information associated with internal routes from site 2 to CSC-CE1. CSC-PE1 also sends the label binding information. As a result, CSC-CE1 gets the route to PE2 with CSC-PE1 as the next hop. The label associated with that route is called L1. |
| 4    | CE1 distributes the routing and labeling information through site 1. Every router in site 1 gets a route for every internal destination in site 2. Therefore, PE1 can establish an MP-IBGP session with PE2.                                                                |
| 5    | CE2 advertises the internal routes of MPLS VPN site 2 to PE2.                                                                                                                                                                                                               |
| 6    | PE2 allocates labels for all the VPN routes (regular MPLS VPN functionality) and advertises it to PE1, using MP-IBGP.                                                                                                                                                       |
| 7    | PE1 can forward traffic from VPN site 1 that is destined for VPN site 2.                                                                                                                                                                                                    |

## How to Configure MPLS VPN CSC with LDP and IGP

This section contains the following procedures:

- [Configuring the Backbone Carrier Core, page 9](#)
- [Configuring the CSC-PE and CSC-CE Routers, page 15](#)
- [Verifying the Carrier Supporting Carrier Configuration, page 17](#)

### Configuring the Backbone Carrier Core

Configuring the backbone carrier core requires setting up connectivity and routing functions for the CSC core and the CSC-PE routers.

Configuring and verifying the CSC core (backbone carrier) involves the following tasks:

- [Verifying IP Connectivity and LDP Configuration in the CSC Core, page 9](#) (optional)
- [Configuring VRFs for CSC-PE Routers, page 11](#) (required)
- [Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier, page 13](#) (required)

### Prerequisites

Before you configure a backbone carrier core, configure the following on the CSC core routers:

- An IGP routing protocol—BGP, OSPF, IS-IS, EIGRP, static, and so on. For information, see the “IP Routing Protocols” chapter in the *Cisco IOS IP Configuration Guide, Release 12.0*.
- Label Distribution Protocol (LDP). For information, see the *MPLS Label Distribution Protocol (LDP)*.

### Verifying IP Connectivity and LDP Configuration in the CSC Core

Perform this task to verify IP connectivity and LDP configuration in the CSC core.

## SUMMARY STEPS

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show mpls forwarding-table** [**vrf** *vrf-name*] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
5. **show mpls ldp discovery** [[**vrf** *vrf-name*] | **all**]
6. **show mpls ldp neighbor** [[**vrf** *vrf-name*] [*address* | *interface*] [**detail**] | **all**]
7. **show ip cef** [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
8. **show mpls interfaces** [[**vrf** *vrf-name*] [*interface*] [**detail**] | **all**]
9. **show ip route**
10. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                     |
| Step 2 | <b>ping</b> [ <i>protocol</i> ] { <i>host-name</i>   <i>system address</i> }<br><br><b>Example:</b><br>Router# ping ip 139.0.0.1                                                                                                                                                                                                                                 | (Optional) Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks. <ul style="list-style-type: none"> <li>Use the <b>ping ip</b> command to verify the connectivity from one CSC core router to another.</li> </ul>                                                                                             |
| Step 3 | <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ]<br><br><b>Example:</b><br>Router# trace ip 139.0.0.1                                                                                                                                                                                                                                                     | (Optional) Discovers the routes that packets will actually take when traveling to their destination. <ul style="list-style-type: none"> <li>Use the <b>trace</b> command to verify the path that a packet goes through before reaching the final destination. The <b>trace</b> command can help isolate a trouble spot if two routers cannot communicate.</li> </ul> |
| Step 4 | <b>show mpls forwarding-table</b> [ <b>vrf</b> <i>vrf-name</i> ] [{ <i>network</i> { <i>mask</i>   <i>length</i> }   <b>labels</b> <i>label</i> [- <i>label</i> ]   <b>interface</b> <i>interface</i>   <b>next-hop</b> <i>address</i>   <b>lsp-tunnel</b> [ <i>tunnel-id</i> ]}] [ <b>detail</b> ]<br><br><b>Example:</b><br>Router# show mpls forwarding-table | (Optional) Displays the contents of the MPLS label forwarding information base (LFIB). <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command to verify that MPLS packets are being forwarded.</li> </ul>                                                                                                                          |
| Step 5 | <b>show mpls ldp discovery</b> [[ <b>vrf</b> <i>vrf-name</i> ]   <b>all</b> ]<br><br><b>Example:</b><br>Router# show mpls ldp discovery                                                                                                                                                                                                                          | (Optional) Displays the status of the LDP discovery process. <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp discovery</b> command to verify that LDP is operational in the CSC core.</li> </ul>                                                                                                                                                     |

|         | Command or Action                                                                                                                                  | Purpose                                                                                                                                                                                                                                                             |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <pre>show mpls ldp neighbor [[vrf vrf-name] [address   interface] [detail]  [all]]</pre> <p><b>Example:</b><br/>Router# show mpls ldp neighbor</p> | (Optional) Displays the status of LDP sessions. <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp neighbor</b> command to verify LDP configuration in the CSC core.</li> </ul>                                                                        |
| Step 7  | <pre>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</pre> <p><b>Example:</b><br/>Router# show ip cef</p>                   | (Optional) Displays entries in the forwarding information base (FIB). <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> command to check the forwarding table (prefixes, next hops, and interfaces).</li> </ul>                                     |
| Step 8  | <pre>show mpls interfaces [[vrf vrf-name] [interface] [detail]  [all]]</pre> <p><b>Example:</b><br/>Router# show mpls interfaces</p>               | (Optional) Displays information about one or more or all interfaces that are configured for label switching. <ul style="list-style-type: none"> <li>Use the <b>show mpls interfaces</b> command to verify that the interfaces are configured to use LDP.</li> </ul> |
| Step 9  | <pre>show ip route</pre> <p><b>Example:</b><br/>Router# show ip route</p>                                                                          | (Optional) Displays IP routing table entries. <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> command to display the entire routing table, including host IP address, next hop, interface, and so forth.</li> </ul>                             |
| Step 10 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                      | (Optional) Returns to privileged EXEC mode.                                                                                                                                                                                                                         |

## Troubleshooting Tips

You can use the **ping** and **trace** commands to verify complete MPLS connectivity in the core. You also get useful troubleshooting information from the additional **show** commands.

## Additional Information

For a configuration example for this task, see the [“Verifying IP Connectivity and LDP Configuration in the CSC Core”](#) section on page 9.

## Configuring VRFs for CSC-PE Routers

Perform this task to configure VPN forwarding/routing instances (VRFs) for the backbone carrier edge (CSC-PE) routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf vrf-name**
4. **rd route-distinguisher**
5. **route-target {import | export | both} route-target-ext-community**

6. **import map** *route-map*
7. **exit**
8. **interface** *type number*
9. **ip vrf forwarding** *vrf-name*
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                       | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                  | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <p><b>ip vrf</b> <i>vrf-name</i></p> <p><b>Example:</b><br/>Router(config)# ip vrf vpn1</p>                                                                                             | <p>Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode.</p> <ul style="list-style-type: none"> <li>• The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 4 | <p><b>rd</b> <i>route-distinguisher</i></p> <p><b>Example:</b><br/>Router(config-vrf)# rd 100:1</p>                                                                                     | <p>Creates routing and forwarding tables.</p> <ul style="list-style-type: none"> <li>• The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN-IPv4 prefix. You can enter an RD in either of these formats: <ul style="list-style-type: none"> <li>– 16-bit AS number: your 32-bit number, for example, 101:3</li> <li>– 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul>                                                                                                                                                                                                                      |
| Step 5 | <p><b>route-target</b> {<b>import</b>   <b>export</b>   <b>both</b>}<br/><i>route-target-ext-community</i></p> <p><b>Example:</b><br/>Router(config-vrf)# route-target import 100:1</p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>• The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>• The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>• The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>• The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |

|         | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                         |
|---------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>import map</b> <i>route-map</i><br><br><b>Example:</b><br>Router(config-vrf)# import map vpn1-route-map   | (Optional) Configures an import route map for a VRF. <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                     |
| Step 7  | <b>exit</b><br><br><b>Example:</b><br>Router(config-vrf)# exit                                               | (Optional) Exits to global configuration mode.                                                                                                                                                                                                                  |
| Step 8  | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet5/0          | Specifies the interface to configure. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul> |
| Step 9  | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1 | Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                    |
| Step 10 | <b>end</b><br><br>Router(config-if)# end                                                                     | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                       |

### Troubleshooting Tips

Enter a **show ip vrf detail** command and make sure the MPLS VPN is up and associated with the right interfaces.

## Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier

Perform this task to configure Multiprotocol BGP (MP-BGP) connectivity in the backbone carrier.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type*
7. **address-family** *vpn4* [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community** **extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                    | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>no bgp default ipv4-unicast</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default ipv4-unicast                                                         | (Optional) Disables the IPv4 unicast address family on all neighbors. <ul style="list-style-type: none"> <li>Use the <b>no</b> form of the <b>bgp default-unicast</b> command if you are using this neighbor for MPLS routes only.</li> </ul>                                                                                                                                                                                            |
| Step 5 | <b>neighbor {ip-address   peer-group-name} remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 139.0.0.1 remote-as 100                    | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                      |
| Step 6 | <b>neighbor {ip-address   peer-group-name} update-source interface-type</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 139.0.0.1 update-source loopback0 | Allows BGP sessions to use a specific operational interface for TCP connections. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument specifies the interface to be used as the source.</li> </ul>                              |
| Step 7 | <b>address-family vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                             | Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                                                        |

|         | Command or Action                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <pre>neighbor {ip-address   peer-group-name} send-community extended</pre> <p><b>Example:</b></p> <pre>Router(config-router-af)# neighbor pp.0.0.1 send-community extended</pre> | <p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 9  | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b></p> <pre>Router(config-router-af)# neighbor &lt;CSC-Core-ip-address&gt; activate</pre>            | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                    |
| Step 10 | <pre>end</pre> <p><b>Example:</b></p> <pre>Router(config-router-af)# end</pre>                                                                                                   | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                             |

### Troubleshooting Tips

You can enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. If this command is not successful, enter a **debug ip bgp x.x.x.x events** command, where *x.x.x.x* is the IP address of the neighbor.

## Configuring the CSC-PE and CSC-CE Routers

To enable the CSC-PE and CSC-CE routers to distribute routes and MPLS labels, perform the following tasks:

- [Configuring an IGP on the CSC-PE and CSC-CE Routers, page 15](#)
- [Configuring LDP on the CSC-PE and CSC-CE Routers, page 15](#)
- [Enabling MPLS Encapsulation on the CSC-PE and CSC-CE Routers, page 16](#)

### Configuring an IGP on the CSC-PE and CSC-CE Routers

A routing protocol is required between the PE and 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. Use the same routing protocol that the customer carrier uses. You can choose RIP, OSPF, or static routing as the routing protocol. BGP is not supported. For the configuration steps, see the [Configuring MPLS Layer 3 VPNs](#) process module.

### Configuring LDP on the CSC-PE and CSC-CE Routers

MPLS label distribution protocol (LDP) is required between the PE and CE routers that connect the backbone carrier to the customer carrier. You can configure LDP as the default label distribution protocol for the entire router or just for the PE-to-CE interface for VPN routing/forwarding (VRF).

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **mpls label protocol ldp**
4. **interface** *type number*
5. **mpls label protocol ldp**
6. **exit**

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                            | <b>Purpose</b>                                                                                                                                                                                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                     |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                      |
| <b>Step 3</b> | <b>mpls label protocol ldp</b><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp    | Specifies MPLS LDP as the default label distribution protocol for the router.                                                                                                                                                                                                                                          |
| <b>Step 4</b> | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet5/0 | (Optional) Specifies the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type</i> argument specifies the type of interface to be configured.</li> <li>• The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul> |
| <b>Step 5</b> | <b>mpls label protocol ldp</b><br><br><b>Example:</b><br>Router(config-if)# mpls label protocol ldp | (Optional) Specifies MPLS LDP as the default label distribution protocol for the interface.                                                                                                                                                                                                                            |
| <b>Step 6</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                       | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                              |

**Enabling MPLS Encapsulation on the CSC-PE and CSC-CE Routers**

Every packet that crosses the backbone carrier must be encapsulated, so that the packet includes MPLS labels. You can enable MPLS encapsulation for the entire router or just on the interface of the PE or CE router. To enable the encapsulation of packets, perform the following task.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **interface** *type number*
5. **mpls ip**
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip                                    | Enables MPLS encapsulation for the router.                                                                                                                                                                                                                                                                             |
| Step 4 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet5/0 | (Optional) Specifies the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type</i> argument specifies the type of interface to be configured.</li> <li>• The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul> |
| Step 5 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                 | (Optional) Enables MPLS encapsulation for the specified interface.                                                                                                                                                                                                                                                     |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                       | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                              |

## Verifying the Carrier Supporting Carrier Configuration

The following commands verify the status of LDP sessions that were configured between the backbone carrier and customer carrier. Now the customer carrier ISP sites appear as a VPN customer to the backbone carrier.

## SUMMARY STEPS

1. **show mpls ldp discovery vrf**
2. **show mpls ldp discovery all**

## DETAILED STEPS

### Step 1 **show mpls ldp discovery vrf**

Use this command to show that the LDP sessions are in VRF VPN1 of the PE router of the backbone carrier, for example:

```
Router# show mpls ldp discovery vrf vpn1

Local LDP Identifier:
 139.0.0.0:0
Discovery Sources:
 Interfaces:
 Ethernet1/0 (ldp): xmit/recv
 LDP Id: 55.0.0.1:0
 POS6/0 (ldp): xmit
```

### Step 2 **show mpls ldp discovery all**

Use this command to list all LDP sessions in a router, for example:

```
Router# show mpls ldp discovery all

Local LDP Identifier:
 141.141.141.141:0
Discovery Sources:
 Interfaces:
 Ethernet1/5 (ldp): xmit/recv
 LDP Id: 5.5.5.5:0
VRF vpn1: Local LDP Identifier:
 139.0.0.1:0
Discovery Sources:
 Interfaces:
 Ethernet1/0 (ldp): xmit/recv
 LDP Id: 55.0.0.1:0
 POS6/0 (ldp): xmit
```

The Local LDP Identifier field shows the LDP identifier for the local label switching router for this session. The Interfaces field displays the interfaces engaging in LDP discovery activity:

- xmit indicates that the interface is transmitting LDP discovery hello packets.
- rcv indicates that the interface is receiving LDP discovery hello packets.

# Configuration Examples for MPLS VPN CSC with LDP and IGP

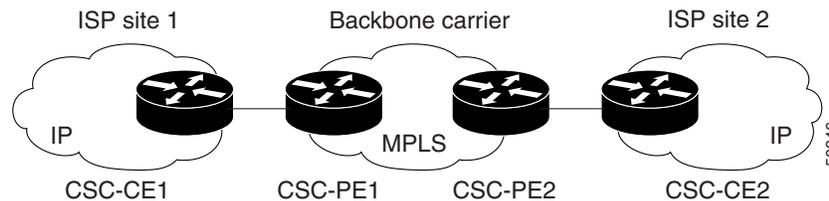
This section provides the following configuration examples:

- [MPLS VPN CSC Network with a Customer Who Is an ISP: Example](#)
- [MPLS VPN CSC Network with a Customer Who Is an MPLS VPN Provider: Example](#)
- [MPLS VPN CSC Network That Contains Route Reflectors: Example](#)
- [MPLS VPN CSC Network with a Customer Who Has VPNs at the Network Edge: Example](#)

## MPLS VPN CSC Network with a Customer Who Is an ISP: Example

Figure 6 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 CE routers that connect the ISPs to the backbone carrier run MPLS.

**Figure 6** Carrier Supporting Carrier Network with a Customer Carrier Who Is an ISP



The following examples show the configuration of each router in the carrier supporting carrier network. OSPF is used to connect the customer carrier to the backbone carrier.

### CSC-CE1 Configuration

```
mpls label protocol ldp
!
interface Loopback0
 ip address 14.14.14.14 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 46.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
```

```

no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
ip address 38.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 14.14.14.14 0.0.0.0 area 200
network 38.0.0.0 0.255.255.255 area 200
network 46.0.0.0 0.255.255.255 area 200

```

## CSC-PE1 Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
ip address 11.11.11.11 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 19.19.19.19 255.255.255.255
no ip directed-broadcast
!
interface ATM1/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1 point-to-point
ip address 33.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0

```

```

no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 46.0.0.1 255.0.0.0
no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 11.11.11.11 0.0.0.0 area 100
 network 33.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 19.19.19.19 0.0.0.0 area 200
 network 46.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 12.12.12.12 remote-as 100
 neighbor 12.12.12.12 update-source Loopback0
!
 address-family ipv4
 neighbor 12.12.12.12 activate
 neighbor 12.12.12.12 send-community extended
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor 12.12.12.12 activate
 neighbor 12.12.12.12 send-community extended
 exit-address-family
!
 address-family ipv4 vrf vpn1
 redistribute ospf 200 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family

```

## CSC-PE2 Configuration

```

ip cef distributed
!
ip vrf vpn1
 rd 100:0
 route-target export 100:0
 route-target import 100:0
 mpls label protocol ldp

```

```

no mpls aggregate-statistics
!
interface Loopback0
 ip address 12.12.12.12 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback100
 ip vrf forwarding vpn1
 ip address 20.20.20.20 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
 ip address 33.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 47.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 12.12.12.12 0.0.0.0 area 100
 network 33.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 20.20.20.20 0.0.0.0 area 200
 network 47.0.0.0 0.255.255.255 area 200
!
router bgp 100

```

```

bgp log-neighbor-changes
timers bgp 10 30
neighbor 11.11.11.11 remote-as 100
neighbor 11.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 11.11.11.11 activate
neighbor 11.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 11.11.11.11 activate
neighbor 11.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE2 Configuration

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address 16.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 47.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 43.0.0.2 255.0.0.0

```

```

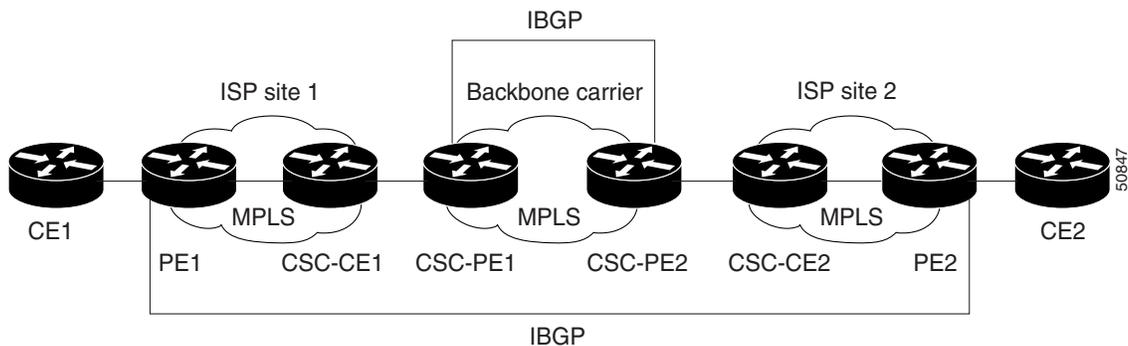
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 16.16.16.16 0.0.0.0 area 200
network 43.0.0.0 0.255.255.255 area 200
network 47.0.0.0 0.255.255.255 area 200

```

## MPLS VPN CSC Network with a Customer Who Is an MPLS VPN Provider: Example

Figure 7 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 7** Carrier Supporting Carrier Network with a Customer Carrier Who Is an MPLS VPN Provider



The following configuration examples show the configuration of each router in the carrier supporting carrier network. OSPF is the protocol used to connect the customer carrier to the backbone carrier.

### CE1 Configuration

```

ip cef
!
interface Loopback0
ip address 17.17.17.17 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/1
ip address 37.0.0.2 255.0.0.0
no ip directed-broadcast
!
router ospf 300
log-adjacency-changes
redistribute bgp 300 subnets
passive-interface Ethernet0/1
network 17.17.17.17 0.0.0.0 area 300

```

```

!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute ospf 300 match internal external 1 external 2
 neighbor 37.0.0.1 remote-as 200
 neighbor 37.0.0.1 advertisement-interval 5
 no auto-summary

```

## PE1 Configuration

```

ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
 ip address 13.13.13.13 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 38.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 37.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 passive-interface Ethernet3/0
 network 13.13.13.13 0.0.0.0 area 200
 network 38.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 15.15.15.15 remote-as 200

```

```

neighbor 15.15.15.15 update-source Loopback0
!
address-family ipv4
neighbor 15.15.15.15 activate
neighbor 15.15.15.15 send-community extended
no synchronization
exit-address-family
!
address-family vpv4
neighbor 15.15.15.15 activate
neighbor 15.15.15.15 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor 37.0.0.2 remote-as 300
neighbor 37.0.0.2 activate
neighbor 37.0.0.2 as-override
neighbor 37.0.0.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE1 Configuration

```

mpls label protocol ldp
!
interface Loopback0
 ip address 14.14.14.14 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 46.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 38.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap

```

```

no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 14.14.14.14 0.0.0.0 area 200
network 38.0.0.0 0.255.255.255 area 200
network 46.0.0.0 0.255.255.255 area 200

```

## CSC-PE1 Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
ip address 11.11.11.11 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 19.19.19.19 255.255.255.255
no ip directed-broadcast
!
interface ATM1/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1 point-to-point
ip address 33.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 46.0.0.1 255.0.0.0
no ip directed-broadcast

```

```

atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 11.11.11.11 0.0.0.0 area 100
network 33.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute bgp 100 metric-type 1 subnets
network 19.19.19.19 0.0.0.0 area 200
network 46.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 12.12.12.12 remote-as 100
neighbor 12.12.12.12 update-source Loopback0
!
address-family ipv4
neighbor 12.12.12.12 activate
neighbor 12.12.12.12 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 12.12.12.12 activate
neighbor 12.12.12.12 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-PE2 Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
ip address 12.12.12.12 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 20.20.20.20 255.255.255.255
no ip directed-broadcast

```

```
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
 ip address 33.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 47.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 12.12.12.12 0.0.0.0 area 100
 network 33.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 20.20.20.20 0.0.0.0 area 200
 network 47.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 11.11.11.11 remote-as 100
 neighbor 11.11.11.11 update-source Loopback0
 !
 address-family ipv4
 neighbor 11.11.11.11 activate
 neighbor 11.11.11.11 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
```

```

neighbor 11.11.11.11 activate
neighbor 11.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE2 Configuration

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address 16.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 47.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 43.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 network 16.16.16.16 0.0.0.0 area 200
 network 43.0.0.0 0.255.255.255 area 200
 network 47.0.0.0 0.255.255.255 area 200

```

## PE2 Configuration

```

ip cef
ip cef accounting non-recursive
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
 ip address 15.15.15.15 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 42.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 43.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 passive-interface Ethernet3/0
 network 15.15.15.15 0.0.0.0 area 200
 network 43.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 13.13.13.13 remote-as 200
 neighbor 13.13.13.13 update-source Loopback0
 !
 address-family ipv4
 neighbor 13.13.13.13 activate
 neighbor 13.13.13.13 send-community extended
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 13.13.13.13 activate
 neighbor 13.13.13.13 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 neighbor 42.0.0.2 remote-as 300

```

```

neighbor 42.0.0.2 activate
neighbor 42.0.0.2 as-override
neighbor 42.0.0.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family

```

## CE2 Configuration

```

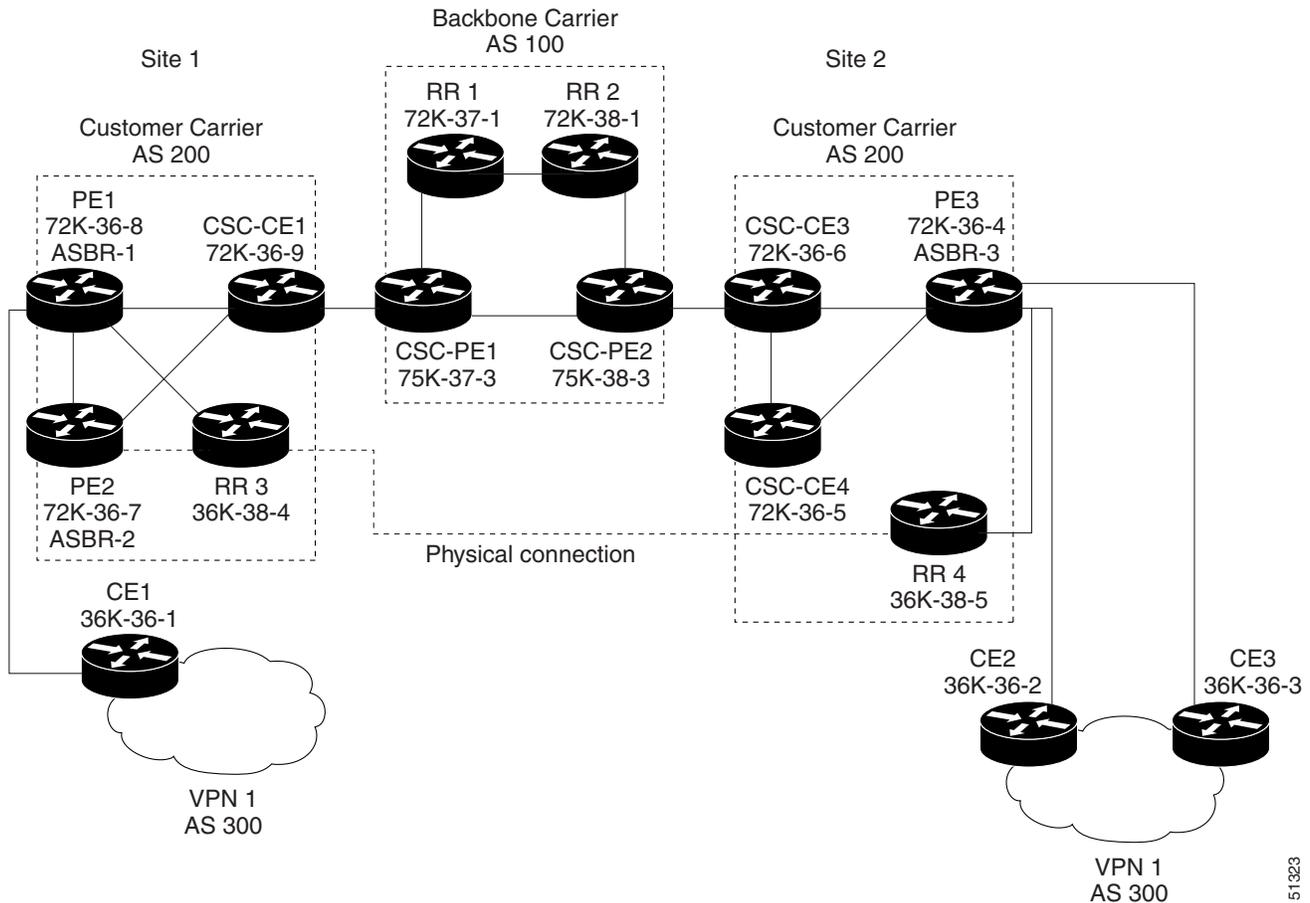
ip cef
!
interface Loopback0
 ip address 18.18.18.18 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 42.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 log-adjacency-changes
 redistribute bgp 300 subnets
 passive-interface Ethernet0/1
 network 18.18.18.18 0.0.0.0 area 300
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute ospf 300 match internal external 1 external 2
 neighbor 42.0.0.1 remote-as 200
 neighbor 42.0.0.1 advertisement-interval 5
 no auto-summary

```

## MPLS VPN CSC Network That Contains Route Reflectors: Example

Figure 8 shows a carrier supporting carrier network configuration that contains route reflectors. The customer carrier has two sites.

**Figure 8** Carrier Supporting Carrier Network that Contains Route Reflectors



**Note**

A connection between route reflectors (RR) is not necessary.

The following configuration examples show the configuration of each router in the carrier supporting carrier network. Note the following:

- The router IP addresses are abbreviated for ease of reading. For example, the loopback address for PE 1 is 25, which is equivalent to 25.25.25.25.
- The following list shows the loopback addresses for the CSC-PE routers:
  - CSC-PE1 (75K-37-3): loopback 0 = 15.15.15.15, loopback 1 = 18.18.18.18
  - CSC-PE2 (75K-38-3): loopback 0 = 16.16.16.16, loopback 1 = 20.20.20.20

## Backbone Carrier Configuration

### Route Reflector 1 (72K-37-1) Configuration

```
interface Loopback0
 ip address 13.13.13.13 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
```

```

!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 mpls
 ip address 51.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM1/1
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1.1 mpls
 ip address 52.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 13.0.0.0 0.255.255.255 area 100
 network 51.0.0.0 0.255.255.255 area 100
 network 52.0.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 1
 redistribute static
 neighbor 15.15.15.15 remote-as 100
 neighbor 15.15.15.15 update-source Loopback0
 neighbor 16.16.16.16 remote-as 100
 neighbor 16.16.16.16 update-source Loopback0
!
 address-family ipv4 vrf vpn1
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor 15.15.15.15 activate
 neighbor 15.15.15.15 route-reflector-client
 neighbor 15.15.15.15 send-community extended
 neighbor 16.16.16.16 activate
 neighbor 16.16.16.16 route-reflector-client
 neighbor 16.16.16.16 send-community extended
 bgp scan-time import 5
 exit-address-family

```

## Route Reflector 2 (72K-38-1) Configuration

```
interface Loopback0
 ip address 14.14.14.14 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 mpls
 ip address 53.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM1/1
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1.1 mpls
 ip address 52.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 14.0.0.0 0.255.255.255 area 100
 network 52.0.0.0 0.255.255.255 area 100
 network 53.0.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 1
 redistribute static
 neighbor 15.15.15.15 remote-as 100
 neighbor 15.15.15.15 update-source Loopback0
 neighbor 16.16.16.16 remote-as 100
 neighbor 16.16.16.16 update-source Loopback0
!
```

```

address-family ipv4 vrf vpn1
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 15.15.15.15 activate
neighbor 15.15.15.15 route-reflector-client
neighbor 15.15.15.15 send-community extended
neighbor 16.16.16.16 activate
neighbor 16.16.16.16 route-reflector-client
neighbor 16.16.16.16 send-community extended
bgp scan-time import 5
exit-address-family

```

### CSC-PE1 (75K-37-3) Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
!
interface Loopback0
ip address 15.15.15.15 255.255.255.255
no ip directed-broadcast
!
interface Loopback1
ip vrf forwarding vpn1
ip address 18.18.18.18 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/0/1
ip vrf forwarding vpn1
ip address 55.0.0.2 255.0.0.0
no ip directed-broadcast
no ip route-cache distributed
mpls label protocol ldp
mpls ip
!
interface ATM1/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1 mpls
ip address 56.0.0.1 255.0.0.0
no ip directed-broadcast
no atm enable-ilmi-trap
mpls label protocol ldp
mpls atm vpi 2-5
mpls ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL

```

```
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 50.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 6 32 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/1/0.1 mpls
ip address 51.0.0.1 255.0.0.0
no ip directed-broadcast
no atm enable-ilmi-trap
mpls label protocol ldp
mpls atm vpi 2-5
mpls ip
!
router ospf 100
auto-cost reference-bandwidth 10000
network 15.0.0.0 0.255.255.255 area 100
network 50.0.0.0 0.255.255.255 area 100
network 51.0.0.0 0.255.255.255 area 100
network 55.0.0.0 0.255.255.255 area 100
network 56.0.0.0 0.255.255.255 area 100
!
router ospf 1 vrf vpn1
redistribute bgp 100 metric-type 1 subnets
network 17.0.0.0 0.255.255.255 area 101
network 18.0.0.0 0.255.255.255 area 101
network 50.0.0.0 0.255.255.255 area 101
network 55.0.0.0 0.255.255.255 area 101
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 13.13.13.13 remote-as 100
neighbor 13.13.13.13 update-source Loopback0
neighbor 14.14.14.14 remote-as 100
neighbor 14.14.14.14 update-source Loopback0
!
address-family ipv4
redistribute static
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 13.13.13.13 activate
neighbor 13.13.13.13 send-community extended
neighbor 14.14.14.14 activate
neighbor 14.14.14.14 send-community extended
exit-address-family
```

```

!
address-family ipv4 vrf vpn1
redistribute ospf 1 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

### CSC-PE2 (75K-38-3) Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
!
interface Loopback0
ip address 16.16.16.16 255.255.255.255
no ip directed-broadcast
!
interface Loopback1
ip vrf forwarding vpn1
ip address 20.20.20.20 255.255.255.255
no ip directed-broadcast
!
interface ATM0/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM0/1/0.1 mpls
ip address 56.0.0.2 255.0.0.0
no ip directed-broadcast
no atm enable-ilmi-trap
mpls label protocol ldp
mpls atm vpi 2-5
mpls ip
!
interface ATM2/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM2/1/0.1 mpls
ip address 53.0.0.2 255.0.0.0
no ip directed-broadcast
no atm enable-ilmi-trap
mpls label protocol ldp
mpls atm vpi 2-5
mpls ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed

```

```
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 54.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 100 6 32 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/1/0.1 point-to-point
ip vrf forwarding vpn1
ip address 57.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 101 6 33 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
auto-cost reference-bandwidth 10000
network 16.0.0.0 0.255.255.255 area 100
network 53.0.0.0 0.255.255.255 area 100
network 54.0.0.0 0.255.255.255 area 100
network 56.0.0.0 0.255.255.255 area 100
network 57.0.0.0 0.255.255.255 area 100
!
router ospf 1 vrf vpn1
redistribute bgp 100 metric-type 1 subnets
network 19.0.0.0 0.255.255.255 area 101
network 20.0.0.0 0.255.255.255 area 101
network 54.0.0.0 0.255.255.255 area 101
network 57.0.0.0 0.255.255.255 area 101
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 13.13.13.13 remote-as 100
neighbor 13.13.13.13 update-source Loopback0
neighbor 14.14.14.14 remote-as 100
neighbor 14.14.14.14 update-source Loopback0
!
address-family ipv4
redistribute static
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 13.13.13.13 activate
neighbor 13.13.13.13 send-community extended
```

```

neighbor 14.14.14.14 activate
neighbor 14.14.14.14 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 1 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## Customer Carrier Site 1 Configuration

### PE1 (72K-36-8) Configuration

```

ip cef
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
no mpls ip propagate-ttl
!
interface Loopback0
ip address 25.25.25.25 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 66.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
mpls label protocol ldp
mpls ip
!
interface Ethernet3/0
ip vrf forwarding vpn2
ip address 70.0.0.1 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet3/1
ip address 67.0.0.1 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/2
ip address 64.0.0.2 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!

```

```

router ospf 1
 network 25.0.0.0 0.255.255.255 area 101
 network 64.0.0.0 0.255.255.255 area 101
 network 66.0.0.0 0.255.255.255 area 101
 network 67.0.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 22.22.22.22 remote-as 200
 neighbor 22.22.22.22 update-source Loopback0
 neighbor 23.23.23.23 remote-as 200
 neighbor 23.23.23.23 update-source Loopback0
!
 address-family ipv4 vrf vpn2
 redistribute connected
 neighbor 70.0.0.2 remote-as 300
 neighbor 70.0.0.2 activate
 neighbor 70.0.0.2 as-override
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor 22.22.22.22 activate
 neighbor 22.22.22.22 send-community extended
 neighbor 23.23.23.23 activate
 neighbor 23.23.23.23 send-community extended
 exit-address-family

```

### CSC-CE1 (72K-36-9) Configuration

```

ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 11.11.11.11 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 50.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 66.0.0.1 255.0.0.0
 no ip directed-broadcast

```

```

 atm pvc 100 0 50 aal5snap
mpls label protocol ldp
mpls ip
!
interface Ethernet3/0
 ip address 65.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/1
 ip address 55.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 11.0.0.0 0.255.255.255 area 101
 network 50.0.0.0 0.255.255.255 area 101
 network 55.0.0.0 0.255.255.255 area 101
 network 65.0.0.0 0.255.255.255 area 101
 network 66.0.0.0 0.255.255.255 area 101

```

## PE2 (72K-36-7) Configuration

```

ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
no mpls ip propagate-ttl
!
interface Loopback0
 ip address 24.24.24.24 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet3/0
 ip address 65.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/1
 ip vrf forwarding vpn2
 ip address 71.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet3/2
 ip address 67.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!

```

```

interface Ethernet3/3
 ip address 63.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 mpls ip
 !
router ospf 1
 network 24.0.0.0 0.255.255.255 area 101
 network 63.0.0.0 0.255.255.255 area 101
 network 65.0.0.0 0.255.255.255 area 101
 network 67.0.0.0 0.255.255.255 area 101
 !
router bgp 200
 neighbor 22.22.22.22 remote-as 200
 neighbor 22.22.22.22 update-source Loopback0
 neighbor 23.23.23.23 remote-as 200
 neighbor 23.23.23.23 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 neighbor 71.0.0.2 remote-as 300
 neighbor 71.0.0.2 activate
 neighbor 71.0.0.2 as-override
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 22.22.22.22 activate
 neighbor 22.22.22.22 send-community extended
 neighbor 23.23.23.23 activate
 neighbor 23.23.23.23 send-community extended
 exit-address-family

```

### Route Reflector 3 (36K-38-4) Configuration

```

ip cef
 !
interface Loopback0
 ip address 23.23.23.23 255.255.255.255
 !
interface Ethernet1/1
 ip address 64.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
 !
interface Ethernet1/2
 ip address 63.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
 !
interface ATM3/0
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
 !
interface ATM3/0.1 point-to-point
 ip address 62.0.0.2 255.0.0.0
 atm pvc 100 0 55 aal5snap
 mpls label protocol ldp
 mpls ip

```

```

!
router ospf 1
 log-adjacency-changes
 network 23.0.0.0 0.255.255.255 area 101
 network 62.0.0.0 0.255.255.255 area 101
 network 63.0.0.0 0.255.255.255 area 101
 network 64.0.0.0 0.255.255.255 area 101
!
router bgp 200
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 2
 redistribute static
 neighbor 21.21.21.21 remote-as 200
 neighbor 21.21.21.21 update-source Loopback0
 neighbor 24.24.24.24 remote-as 200
 neighbor 24.24.24.24 update-source Loopback0
 neighbor 25.25.25.25 remote-as 200
 neighbor 25.25.25.25 update-source Loopback0
!
 address-family ipv4 vrf vpn2
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 21.21.21.21 activate
 neighbor 21.21.21.21 route-reflector-client
 neighbor 21.21.21.21 send-community extended
 neighbor 24.24.24.24 activate
 neighbor 24.24.24.24 route-reflector-client
 neighbor 24.24.24.24 send-community extended
 neighbor 25.25.25.25 activate
 neighbor 25.25.25.25 route-reflector-client
 neighbor 25.25.25.25 send-community extended
 exit-address-family

```

### CE1 (36K-36-1) Configuration

```

ip cef
!
interface Loopback0
 ip address 28.28.28.28 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 70.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet0/2
 ip address 71.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router bgp 300
 network 28.0.0.0
 network 70.0.0.0
 network 71.0.0.0
 neighbor 70.0.0.1 remote-as 200
 neighbor 71.0.0.1 remote-as 200

```

## Customer Carrier Site 2 Configuration

### CSC-CE3 (72K-36-6) Configuration

```

ip cef
!
interface Loopback0
 ip address 12.12.12.12 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 54.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
 mpls label protocol ldp

 mpls ip
!
interface POS2/0
 ip address 58.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 59.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 40 aal5snap
 mpls ip
!
router ospf 1
 network 12.0.0.0 0.255.255.255 area 101
 network 54.0.0.0 0.255.255.255 area 101
 network 58.0.0.0 0.255.255.255 area 101
 network 59.0.0.0 0.255.255.255 area 101

```

### PE3 (72K-36-4) Configuration

```

ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
!

```

```

!
interface Loopback0
 ip address 21.21.21.21 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 80.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet3/1
 ip vrf forwarding vpn2
 ip address 81.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet3/2
 ip address 61.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 59.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 40 aal5snap
 mpls label protocol ldp
 mpls ip
!
interface ATM6/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
 ip address 60.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 20 aal5snap
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 network 21.0.0.0 0.255.255.255 area 101
 network 59.0.0.0 0.255.255.255 area 101
 network 60.0.0.0 0.255.255.255 area 101
 network 61.0.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 22.22.22.22 remote-as 200
 neighbor 22.22.22.22 update-source Loopback0
 neighbor 23.23.23.23 remote-as 200
 neighbor 23.23.23.23 update-source Loopback0
!
 address-family ipv4 vrf vpn2
 redistribute connected
 neighbor 80.0.0.2 remote-as 300
 neighbor 80.0.0.2 activate
 neighbor 80.0.0.2 as-override

```

```
neighbor 81.0.0.2 remote-as 300
neighbor 81.0.0.2 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 22.22.22.22 activate
neighbor 22.22.22.22 send-community extended
neighbor 23.23.23.23 activate
neighbor 23.23.23.23 send-community extended
exit-address-family
```

### CSC-CE4 (72K-36-5) Configuration

```
ip cef
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
 no ip directed-broadcast
!
interface POS4/0
 ip address 58.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls ip
 clock source internal
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 60.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 20 aal5snap
 mpls label protocol ldp
 mpls ip
!
interface ATM6/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
 ip address 57.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 33 aal5snap
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 57.0.0.0 0.255.255.255 area 101
 network 58.0.0.0 0.255.255.255 area 101
 network 60.0.0.0 0.255.255.255 area 101
```

**Route Reflector 4 (36K-38-5) Configuration**

```

ip cef
!
interface Loopback0
 ip address 22.22.22.22 255.255.255.255
!
interface Ethernet0/1
 ip address 61.0.0.2 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 62.0.0.1 255.0.0.0
 atm pvc 100 0 55 aal5snap
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 22.0.0.0 0.255.255.255 area 101
 network 61.0.0.0 0.255.255.255 area 101
 network 62.0.0.0 0.255.255.255 area 101
!
router bgp 200
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 2
 redistribute static
 neighbor 21.21.21.21 remote-as 200
 neighbor 21.21.21.21 update-source Loopback0
 neighbor 24.24.24.24 remote-as 200
 neighbor 24.24.24.24 update-source Loopback0
 neighbor 25.25.25.25 remote-as 200
 neighbor 25.25.25.25 update-source Loopback0
!
 address-family ipv4 vrf vpn2
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor 21.21.21.21 activate
 neighbor 21.21.21.21 route-reflector-client
 neighbor 21.21.21.21 send-community extended
 neighbor 24.24.24.24 activate
 neighbor 24.24.24.24 route-reflector-client
 neighbor 24.24.24.24 send-community extended
 neighbor 25.25.25.25 activate
 neighbor 25.25.25.25 route-reflector-client
 neighbor 25.25.25.25 send-community extended
 exit-address-family

```

### CE2 (36K-36-2) Configuration

```
ip cef
!
interface Loopback0
 ip address 26.26.26.26 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 80.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet0/2
 ip address 82.0.0.1 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 redistribute bgp 300
 network 26.0.0.0 0.255.255.255 area 300
 network 82.0.0.0 0.255.255.255 area 300
!
router bgp 300
 network 26.0.0.0
 network 80.0.0.0
 network 82.0.0.0
 neighbor 80.0.0.1 remote-as 200
```

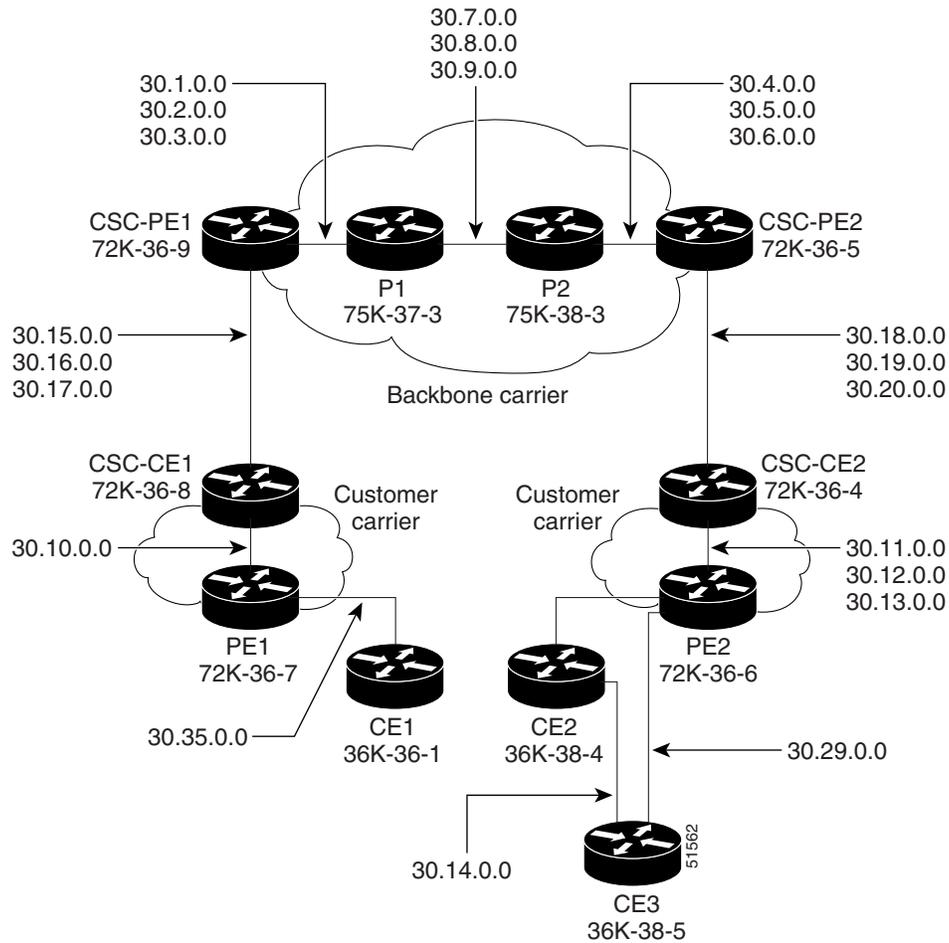
### CE3 (36K-36-3) Configuration

```
ip cef
!
interface Loopback0
 ip address 27.27.27.27 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet1/1
 ip address 81.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet1/2
 ip address 82.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 redistribute bgp 300
 network 27.0.0.0 0.255.255.255 area 300
 network 82.0.0.0 0.255.255.255 area 300
!
router bgp 300
 network 27.0.0.0
 network 81.0.0.0
 network 82.0.0.0
 neighbor 81.0.0.1 remote-as 200
```

## MPLS VPN CSC Network with a Customer Who Has VPNs at the Network Edge: Example

Figure 9 shows a carrier supporting carrier network configuration where the customer carrier has VPNs at the network edge.

Figure 9 Carrier Supporting Carrier Network



## Backbone Carrier Configuration

### CSC-PE1 (72K-36-9) Configuration

```

ip cef
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
!
!
interface Loopback0
ip address 14.14.14.14 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1

```

```
ip address 22.22.22.22 255.255.255.255
no ip directed-broadcast
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 30.1.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.2 point-to-point
ip address 30.2.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.3 point-to-point
ip address 30.3.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
ip vrf forwarding vpn1
ip address 30.15.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0.2 point-to-point
ip vrf forwarding vpn1
ip address 30.16.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0.3 point-to-point
ip vrf forwarding vpn1
ip address 30.17.0.2 255.255.0.0
```

```

no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
passive-interface ATM2/0.1
passive-interface ATM2/0.2
passive-interface ATM2/0.3
passive-interface Loopback100
network 14.14.14.14 0.0.0.0 area 100
network 30.1.0.0 0.0.255.255 area 100
network 30.2.0.0 0.0.255.255 area 100
network 30.3.0.0 0.0.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute connected subnets
redistribute bgp 100 metric-type 1 subnets
network 22.22.22.22 0.0.0.0 area 200
network 30.15.0.0 0.0.255.255 area 200
network 30.16.0.0 0.0.255.255 area 200
network 30.17.0.0 0.0.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 11.11.11.11 remote-as 100
neighbor 11.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 11.11.11.11 activate
neighbor 11.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 11.11.11.11 activate
neighbor 11.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

**P1 (75K-37-3) Configuration**

```
ip cef distributed
!
mpls label protocol ldp
!
interface Loopback0
ip address 12.12.12.12 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1 point-to-point
ip address 30.7.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 103 0 53 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/1/0.2 point-to-point
ip address 30.8.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 104 0 54 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/1/0.3 point-to-point
ip address 30.9.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 105 0 55 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip address 30.1.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls accounting experimental input
tag-switching ip
!
interface ATM3/0/0.2 point-to-point
```

```

ip address 30.2.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/0/0.3 point-to-point
ip address 30.3.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
network 12.12.12.12 0.0.0.0 area 100
network 30.1.0.0 0.0.255.255 area 100
network 30.2.0.0 0.0.255.255 area 100
network 30.3.0.0 0.0.255.255 area 100
network 30.7.0.0 0.0.255.255 area 100
network 30.8.0.0 0.0.255.255 area 100
network 30.9.0.0 0.0.255.255 area 100

```

## P2 (75K-38-3) Configuration

```

ip cef distributed
!
mpls label protocol ldp
!
interface Loopback0
ip address 13.13.13.13 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM0/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
ip address 30.7.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 103 0 53 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM0/1/0.2 point-to-point
ip address 30.8.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 104 0 54 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!

```

```

interface ATM0/1/0.3 point-to-point
ip address 30.9.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 105 0 55 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/1/0.1 point-to-point
ip address 30.4.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0.2 point-to-point
ip address 30.5.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0.3 point-to-point
ip address 30.6.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
network 13.13.13.13 0.0.0.0 area 100
network 30.4.0.0 0.0.255.255 area 100
network 30.5.0.0 0.0.255.255 area 100
network 30.6.0.0 0.0.255.255 area 100
network 30.7.0.0 0.0.255.255 area 100
network 30.8.0.0 0.0.255.255 area 100
network 30.9.0.0 0.0.255.255 area 100
!

```

### CSC-PE2 (72K-36-5) Configuration

```

ip cef
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
!

```

```

interface Loopback0
ip address 11.11.11.11 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 23.23.23.23 255.255.255.255
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip vrf forwarding vpn1
ip address 30.18.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip vrf forwarding vpn1
ip address 30.19.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip vrf forwarding vpn1
ip address 30.20.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
ip address 30.4.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!

```

```
interface ATM6/0.2 point-to-point
ip address 30.5.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.3 point-to-point
ip address 30.6.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
passive-interface ATM5/0.1
passive-interface ATM5/0.2
passive-interface ATM5/0.3
passive-interface Loopback100
network 11.11.11.11 0.0.0.0 area 100
network 30.4.0.0 0.0.255.255 area 100
network 30.5.0.0 0.0.255.255 area 100
network 30.6.0.0 0.0.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute connected subnets
redistribute bgp 100 metric-type 1 subnets
network 23.23.23.23 0.0.0.0 area 200
network 30.18.0.0 0.0.255.255 area 200
network 30.19.0.0 0.0.255.255 area 200
network 30.20.0.0 0.0.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 14.14.14.14 remote-as 100
neighbor 14.14.14.14 update-source Loopback0
!
address-family ipv4
neighbor 14.14.14.14 activate
neighbor 14.14.14.14 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 14.14.14.14 activate
neighbor 14.14.14.14 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

## Customer Carrier Site 1 Configuration

### CSC-CE1 (72K-36-8) Configuration

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
ip address 15.15.15.15 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 30.15.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.2 point-to-point
ip address 30.16.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.3 point-to-point
ip address 30.17.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface Ethernet3/1
ip address 30.10.0.2 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 15.15.15.15 0.0.0.0 area 200
network 30.10.0.0 0.0.255.255 area 200
network 30.15.0.0 0.0.255.255 area 200
network 30.16.0.0 0.0.255.255 area 200
network 30.17.0.0 0.0.255.255 area 200

```

**PE1 (72K-36-7) Configuration**

```
ip cef
!
ip vrf customersite
rd 200:1
route-target export 200:1
route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
ip address 16.16.16.16 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Ethernet3/1
ip vrf forwarding customersite
ip address 30.35.0.2 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet3/2
ip address 30.10.0.1 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
passive-interface Ethernet3/1
network 16.16.16.16 0.0.0.0 area 200
network 30.10.0.0 0.0.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30
neighbor 18.18.18.18 remote-as 200
neighbor 18.18.18.18 update-source Loopback0
!
address-family ipv4
neighbor 18.18.18.18 activate
neighbor 18.18.18.18 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 18.18.18.18 activate
neighbor 18.18.18.18 send-community extended
exit-address-family
!
address-family ipv4 vrf customersite
neighbor 30.35.0.1 remote-as 300
neighbor 30.35.0.1 activate
neighbor 30.35.0.1 as-override
neighbor 30.35.0.1 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family
```

**CE1 (36K-36-1) Configuration**

```

ip cef
!
interface Loopback0
ip address 19.19.19.19 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/2
ip address 30.35.0.1 255.255.0.0
no ip directed-broadcast
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet0/2
network 19.19.19.19 0.0.0.0 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 30.35.0.2 remote-as 200
neighbor 30.35.0.2 advertisement-interval 5
no auto-summary

```

**Customer Carrier Site 2 Configuration****CSC-CE2 (72K-36-4) Configuration**

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
ip address 17.17.17.17 255.255.255.255
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip address 30.11.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip address 30.12.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap

```

```

mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip address 30.13.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0
no ip address
no ip directed-broadcast
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
ip address 30.18.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.2 point-to-point
ip address 30.19.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.3 point-to-point
ip address 30.20.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 17.17.17.17 0.0.0.0 area 200
network 30.11.0.0 0.0.255.255 area 200
network 30.12.0.0 0.0.255.255 area 200
network 30.13.0.0 0.0.255.255 area 200
network 30.18.0.0 0.0.255.255 area 200
network 30.19.0.0 0.0.255.255 area 200
network 30.20.0.0 0.0.255.255 area 200

```

## PE2 (72K-36-6) Configuration

```

ip cef
!
ip vrf customersite
rd 200:1
route-target export 200:1
route-target import 200:1
mpls label protocol ldp

```

```

!
interface Loopback0
ip address 18.18.18.18 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Ethernet3/0
ip vrf forwarding customersite
ip address 30.29.0.2 255.255.0.0
no ip directed-broadcast
!
interface Ethernet3/1
ip vrf forwarding customersite
ip address 30.30.0.2 255.255.0.0
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip address 30.11.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip address 30.12.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip address 30.13.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
passive-interface Ethernet3/0
passive-interface Ethernet3/1
network 18.18.18.18 0.0.0.0 area 200
network 30.11.0.0 0.0.255.255 area 200
network 30.12.0.0 0.0.255.255 area 200
network 30.13.0.0 0.0.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30

```

```

neighbor 16.16.16.16 remote-as 200
neighbor 16.16.16.16 update-source Loopback0
!
address-family ipv4
neighbor 16.16.16.16 activate
neighbor 16.16.16.16 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 16.16.16.16 activate
neighbor 16.16.16.16 send-community extended
exit-address-family
!
address-family ipv4 vrf customersite
neighbor 30.29.0.1 remote-as 300
neighbor 30.29.0.1 activate
neighbor 30.29.0.1 as-override
neighbor 30.29.0.1 advertisement-interval 5
neighbor 30.30.0.1 remote-as 300
neighbor 30.30.0.1 activate
neighbor 30.30.0.1 as-override
neighbor 30.30.0.1 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family

```

### CE2 (36K-38-4) Configuration

```

ip cef
!
interface Loopback0
ip address 21.21.21.21 255.255.255.255
!
interface Ethernet1/3
ip address 30.29.0.1 255.255.0.0
!
interface Ethernet5/0
ip address 30.14.0.1 255.255.0.0
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet1/3
network 21.21.21.21 0.0.0.0 area 300
network 30.14.0.0 0.0.255.255 area 300
!
router bgp 300
no synchronization
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 30.29.0.2 remote-as 200
neighbor 30.29.0.2 advertisement-interval 5
no auto-summary

```

**CE3 (36K-38-5) Configuration**

```
ip cef
!
interface Loopback0
ip address 20.20.20.20 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/2
ip address 30.30.0.1 255.255.0.0
no ip directed-broadcast
!
interface Ethernet0/3
ip address 30.14.0.2 255.255.0.0
no ip directed-broadcast
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet0/2
network 20.20.20.20 0.0.0.0 area 300
network 30.14.0.0 0.0.255.255 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 30.30.0.2 remote-as 200
neighbor 30.30.0.2 advertisement-interval 5
no auto-summary
```

## Additional References

The following sections provide references related to MPLS VPNs.

### Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

### RFCs

| RFC      | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

### Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for MPLS VPN CSC with LDP and IGP

[Table 4](#) lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



#### Note

[Table 4](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 4** Feature Information for MPLS VPN CSC with LDP and IGP

| Feature Name                        | Releases                                                                     | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN Carrier Supporting Carrier | 12.0(14)ST<br>12.0(16)ST<br>12.2(8)T<br>12.0(21)ST<br>12.0(22)S<br>12.0(23)S | This feature enables you to set up and create an MPLS VPN CSC network that uses LDP to transport MPLS labels and an IGP to transport routes.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">Information About MPLS VPN CSC with LDP and IGP, page 3</a></li> <li><a href="#">How to Configure MPLS VPN CSC with LDP and IGP, page 9</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS VPN Carrier Supporting Carrier with BGP

---

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Carrier Supporting Carrier (CSC) enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. This module explains how to configure an MPLS VPN CSC network that uses Border Gateway Protocol (BGP) to distribute routes and MPLS labels.

## Module History

This module was first published on May 2, 2005 and last updated on May 2, 2005.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for MPLS VPN CSC with BGP”](#) section on page 51.

## Contents

- [Prerequisites for MPLS VPN CSC with BGP, page 1](#)
- [Restrictions for MPLS VPN CSC with BGP, page 2](#)
- [Information About MPLS VPN CSC with BGP, page 2](#)
- [How to Configure MPLS VPN CSC with BGP, page 5](#)
- [Configuration Examples for MPLS VPN CSC with BGP, page 34](#)
- [Additional References, page 49](#)
- [Feature Information for MPLS VPN CSC with BGP, page 51](#)

## Prerequisites for MPLS VPN CSC with BGP

You should be able to configure MPLS VPNs with end-to-end (CE-to-CE router) pings working. To accomplish this, you need to know how to configure Interior Gateway Protocols (IGPs), MPLS Label Distribution Protocol (LDP), and Multiprotocol Border Gateway Protocol (MP-BGP).



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Make sure that the CSC-PE routers and the CSC-CE routers run images that support BGP label distribution. Otherwise, you cannot run external BGP (EBGP) between them. Ensure connectivity between the customer carrier and the backbone carrier. EBGP-based label distribution is configured on these links to enable MPLS between the customer and backbone carriers.

## Restrictions for MPLS VPN CSC with BGP

On a provider edge (PE) router, you can configure an interface for either BGP with labels or LDP. You cannot enable both types of label distribution on the same interface. If you switch from one protocol to the other, then you must disable the existing protocol on all interfaces before enabling the other protocol.

This feature does not support the following:

- EBGP multihop between CSC-PE and CSC-CE routers
- EIBGP multipath load sharing

The physical interfaces that connect the BGP speakers must support Cisco Express Forwarding (CEF) or distributed CEF (dCEF) and MPLS.

## Information About MPLS VPN CSC with BGP

Before configuring MPLS VPN CSC, you should understand the following concepts:

- [MPLS VPN CSC Introduction, page 2](#)
- [Benefits of Implementing MPLS VPN CSC, page 3](#)
- [Benefits of Implementing MPLS VPN CSC with BGP, page 3](#)
- [Configuration Options for MPLS VPN CSC with BGP, page 4](#)

## MPLS VPN CSC Introduction

Carrier supporting carrier is a term used to describe a situation where one service provider allows another service provider 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.

A backbone carrier offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services. The customer carrier can be either:

- An Internet service provider (ISP)
- A BGP/MPLS VPN service provider

This document uses the following terminology:

- *CE router*: A customer edge router is part of a customer network and interfaces to a provider edge (PE) router. In this document, the CE router sits on the edge of the customer carrier network.
- *PE router*: A provider edge router is part of a service provider's network connected to a customer edge (CE) router. In this document, the PE router sits on the edge of the backbone carrier network.
- *ASBR*: An autonomous system boundary router connects one autonomous system to another.

## Benefits of Implementing MPLS VPN CSC

The MPLS VPN CSC network provides the following benefits to service providers who are backbone carriers and to customer carriers.

### Benefits to the Backbone Carrier

- The backbone carrier can accommodate many customer carriers and give them access to its backbone. The backbone carrier does not need to create and maintain separate backbones for its customer carriers. Using one backbone network to support multiple customer carriers simplifies the backbone carrier's VPN operations. The backbone carrier uses a consistent method for managing and maintaining the backbone network. This is also cheaper and more efficient than maintaining separate backbones.
- The MPLS VPN carrier supporting carrier feature is scalable. Carrier supporting carrier can change the VPN to meet changing bandwidth and connectivity needs. The feature can accommodate unplanned growth and changes. The carrier supporting carrier feature enables tens of thousands of VPNs to be set up over the same network, and it allows a service provider to offer both VPN and Internet services.
- The MPLS VPN carrier supporting carrier feature is a flexible solution. The backbone carrier can accommodate many types of customer carriers. The backbone carrier can accept customer carriers who are ISPs or VPN service providers or both. The backbone carrier can accommodate customer carriers that require security and various bandwidths.

### Benefits to the Customer Carriers

- The MPLS VPN carrier supporting carrier feature removes from the customer carrier the burden of configuring, operating, and maintaining its own backbone. The customer carrier uses the backbone network of a backbone carrier, but the backbone carrier is responsible for network maintenance and operation.
- Customer carriers who use the VPN services provided by the backbone carrier receive the same level of security that Frame Relay or ATM-based VPNs provide. Customer carriers can also use IPSec in their VPNs for a higher level of security; it is completely transparent to the backbone carrier.
- Customer carriers can use any link layer technology (SONET, DSL, Frame Relay, and so on) to connect the CE routers to the PE routers and the PE routers to the P routers. The MPLS VPN carrier supporting carrier feature is link layer independent. The CE routers and PE routers use IP to communicate, and the backbone carrier uses MPLS.
- The customer carrier can use any addressing scheme and still be supported by a backbone carrier. The customer address space and routing information are independent of the address space and routing information of other customer carriers or the backbone provider.

## Benefits of Implementing MPLS VPN CSC with BGP

You can configure your CSC network to enable BGP to transport routes and MPLS labels between the backbone carrier PE routers and the customer carrier CE routers using multiple paths. The benefits of using BGP to distribute IPv4 routes and MPLS label routes are:

- 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.

## Configuration Options for MPLS VPN CSC with BGP

The backbone carrier offers BGP and MPLS VPN services. The customer carrier can be either of the following:

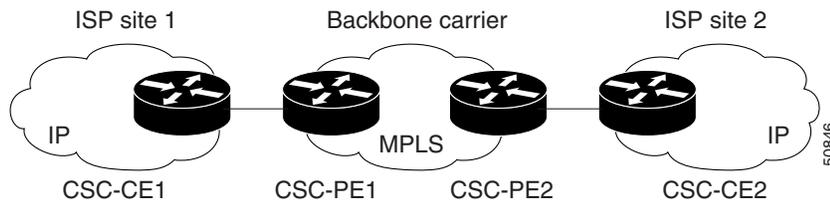
- [Customer Carrier Is an ISP with an IP Core, page 4](#)
- [Customer Carrier Is an MPLS Service Provider With or Without VPN Services, page 5](#)

The following sections explain how the backbone and customer carriers distribute IPv4 routes and MPLS labels.

### Customer Carrier Is an ISP with an IP Core

[Figure 1](#) shows a 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.

**Figure 1** Network Where the Customer Carrier Is an ISP



The links between the CE and PE routers use EBGP to distribute IPv4 routes and MPLS labels. Between the links, the PE routers use multiprotocol IBGP to distribute VPNv4 routes.



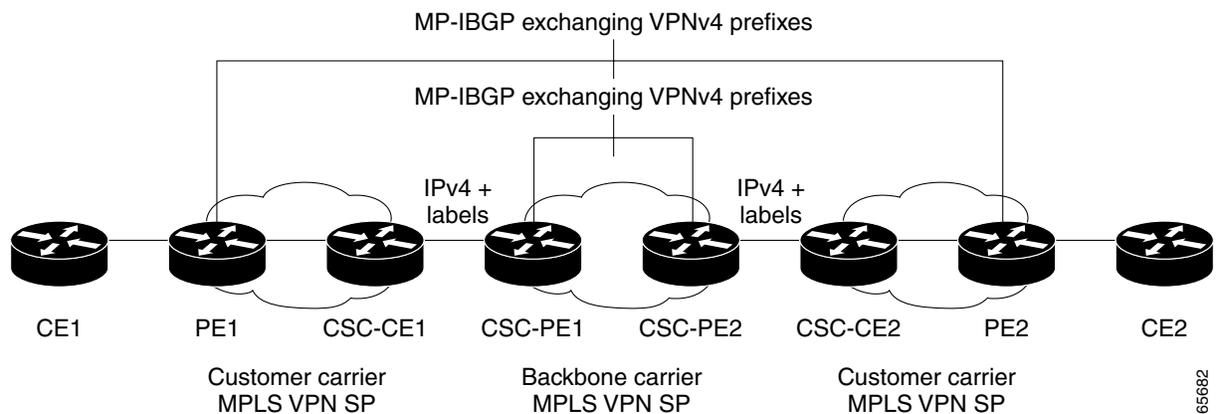
#### Note

If a router other than a Cisco router is used as a CSC-PE or CSC-CE, that router must support IPv4 BGP label distribution (RFC 3107). Otherwise, you cannot run EBGP with labels between the routers.

## Customer Carrier Is an MPLS Service Provider With or Without VPN Services

Figure 2 shows a network configuration where the backbone carrier and the customer carrier are BGP/MPLS VPN service providers. This is known as hierarchical VPNs. The customer carrier has two sites. Both the backbone carrier and the customer carrier use MPLS in their networks.

**Figure 2** Network Where the Customer Carrier Is an MPLS VPN Service Provider



In this configuration, the customer carrier can configure its network in one of the following ways:

- The customer carrier can run IGP and LDP in its core network. In this case, the CSC-CE1 router in the customer carrier redistributes the EBGP routes it learns from the CSC-PE1 router of the backbone carrier to IGP.
- The CSC-CE1 router of the customer carrier system can run an IPv4 and labels IBGP session with the PE1 router.

## How to Configure MPLS VPN CSC with BGP

This section includes the following configuration tasks:

- [Identifying the Carrier Supporting Carrier Topology, page 5](#) (required)
- [Configuring the Backbone Carrier Core, page 6](#) (required)
- [Configuring the CSC-PE and CSC-CE Routers, page 13](#) (required)
- [Configuring the Customer Carrier Network, page 22](#) (required)
- [Configuring the Customer Site for Hierarchical VPNs, page 25](#) (required)

## Identifying the Carrier Supporting Carrier Topology

Before you configure the MPLS VPN CSC with BGP, you need to identify both the backbone and customer carrier topology.

For hierarchical VPNs, the customer carrier of the MPLS VPN network provides MPLS VPN services to its own customers. In this instance, you need to identify the type of customer carrier as well as the topology of the customer carriers. Hierarchical VPNs require extra configuration steps, which are noted in the configuration sections.

**Note**

You can connect multiple CSC-CE routers to the same PE, or you can connect a single CSC-CE router to CSC-PEs using more than one interface to provide redundancy and multiple path support in CSC topology.

Perform this task to identify the carrier supporting carrier topology.

**SUMMARY STEPS**

1. Identify the type of customer carrier, ISP or MPLS VPN service provider.
2. (For hierarchical VPNs only) Identify the CE routers.
3. (For hierarchical VPNs only) Identify the customer carrier core router configuration.
4. Identify the customer carrier edge (CSC-CE) routers.
5. Identify backbone carrier router configuration.

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                              | <b>Purpose</b>                                                                                                                                                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Identify the type of customer carrier, ISP or MPLS VPN service provider.              | Sets up requirements for configuration of carrier supporting carrier network. <ul style="list-style-type: none"> <li>• For an ISP, customer site configuration is not required.</li> <li>• For an MPLS VPN service provider, the customer site needs to be configured, as well as any task or step designated “for hierarchical VPNs only.”</li> </ul> |
| <b>Step 2</b> | (For hierarchical VPNs only) Identify the CE routers.                                 | Sets up requirements for configuration of CE to PE connections.                                                                                                                                                                                                                                                                                        |
| <b>Step 3</b> | (For hierarchical VPNs only) Identify the customer carrier core router configuration. | Sets up requirements for connection configuration between core (P) routers and between P routers and edge routers (PE and CSC-CE routers).                                                                                                                                                                                                             |
| <b>Step 4</b> | Identify the customer carrier edge (CSC-CE) routers.                                  | Sets up requirements for configuration of CSC-CE to CSC-PE connections.                                                                                                                                                                                                                                                                                |
| <b>Step 5</b> | Identify the backbone carrier router configuration.                                   | Sets up requirements for connection configuration between CSC core routers and between CSC core routers and edge routers (CSC-CE and CSC-PE routers).                                                                                                                                                                                                  |

**What to Do Next**

Set up your carrier supporting carrier networks with the [“Configuring the Backbone Carrier Core” section on page 6](#).

**Configuring the Backbone Carrier Core**

Configuring the backbone carrier core requires setting up connectivity and routing functions for the CSC core and the CSC-PE routers.

Configuring and verifying the CSC core (backbone carrier) involves the following tasks:

- [Verifying IP Connectivity and LDP Configuration in the CSC Core, page 7](#) (optional)
- [Configuring VRFs for CSC-PE Routers, page 9](#) (required)
- [Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier, page 11](#) (required)

## Prerequisites

Before you configure a backbone carrier core, configure the following on the CSC core routers:

- An IGP routing protocol—BGP, OSPF, IS-IS, EIGRP, static, and so on.
- Label Distribution Protocol (LDP). For information, see [Configuring MPLS Label Distribution Protocol \(LDP\)](#).

## Verifying IP Connectivity and LDP Configuration in the CSC Core

Perform this task to verify IP connectivity and LDP configuration in the CSC core.

### SUMMARY STEPS

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show mpls forwarding-table** [**vrf** *vrf-name*] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
5. **show mpls ldp discovery** [[**vrf** *vrf-name*] | **all**]
6. **show mpls ldp neighbor** [[**vrf** *vrf-name*] [*address* | *interface*] [**detail**] | **all**]
7. **show ip cef** [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
8. **show mpls interfaces** [[**vrf** *vrf-name*] [*interface*] [**detail**] | **all**]
9. **show ip route**
10. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                                  | Purpose                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                         |
| Step 2 | <b>ping</b> [ <i>protocol</i> ] { <i>host-name</i>   <i>system address</i> }<br><br><b>Example:</b><br>Router# ping ip aa.aa.aa.aa | (Optional) Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks. <ul style="list-style-type: none"> <li>• Use the <b>ping ip</b> command to verify the connectivity from one CSC core router to another.</li> </ul> |

|         | Command or Action                                                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3  | <pre>trace [protocol] [destination]</pre> <p><b>Example:</b><br/>Router# trace ip bb.bb.bb.bb</p>                                                                                                                                                       | <p>(Optional) Discovers the routes that packets will actually take when traveling to their destination.</p> <ul style="list-style-type: none"> <li>Use the <b>trace</b> command to verify the path that a packet goes through before reaching the final destination. The <b>trace</b> command can help isolate a trouble spot if two routers cannot communicate.</li> </ul> |
| Step 4  | <pre>show mpls forwarding-table [vrf vrf-name] [<i>network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]</i>] [detail]</pre> <p><b>Example:</b><br/>Router# show mpls forwarding-table</p> | <p>(Optional) Displays the contents of the MPLS label forwarding information base (LFIB).</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command to verify that MPLS packets are being forwarded.</li> </ul>                                                                                                                          |
| Step 5  | <pre>show mpls ldp discovery [[vrf vrf-name]   [all]]</pre> <p><b>Example:</b><br/>Router# show mpls ldp discovery</p>                                                                                                                                  | <p>(Optional) Displays the status of the LDP discovery process.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp discovery</b> command to verify that LDP is operational in the CSC core.</li> </ul>                                                                                                                                                     |
| Step 6  | <pre>show mpls ldp neighbor [[vrf vrf-name] [address   interface] [detail]   [all]]</pre> <p><b>Example:</b><br/>Router# show mpls ldp neighbor</p>                                                                                                     | <p>(Optional) Displays the status of LDP sessions.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp neighbor</b> command to verify LDP configuration in the CSC core.</li> </ul>                                                                                                                                                                         |
| Step 7  | <pre>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</pre> <p><b>Example:</b><br/>Router# show ip cef</p>                                                                                                                        | <p>(Optional) Displays entries in the forwarding information base (FIB).</p> <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> command to check the forwarding table (prefixes, next hops, and interfaces).</li> </ul>                                                                                                                                      |
| Step 8  | <pre>show mpls interfaces [[vrf vrf-name] [interface] [detail]   [all]]</pre> <p><b>Example:</b><br/>Router# show mpls interfaces</p>                                                                                                                   | <p>(Optional) Displays information about one or more or all interfaces that are configured for label switching.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls interfaces</b> command to verify that the interfaces are configured to use LDP.</li> </ul>                                                                                                  |
| Step 9  | <pre>show ip route</pre> <p><b>Example:</b><br/>Router# show ip route</p>                                                                                                                                                                               | <p>(Optional) Displays IP routing table entries.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> command to display the entire routing table, including host IP address, next hop, interface, and so forth.</li> </ul>                                                                                                                              |
| Step 10 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                                           | <p>(Optional) Returns to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                          |

## Troubleshooting Tips

You can use the **ping** and **trace** commands to verify complete MPLS connectivity in the core. You also get useful troubleshooting information from the additional **show** commands.

## Additional Information

For a configuration example for this task, see the [“Verifying IP Connectivity and LDP Configuration in the CSC Core: Example”](#) section on page 35.

## Configuring VRFs for CSC-PE Routers

Perform this task to configure VPN forwarding/routing instances (VRFs) for the backbone carrier edge (CSC-PE) routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map** *route-map*
7. **exit**
8. **interface** *type number*
9. **ip vrf forwarding** *vrf-name*
10. **end**

### DETAILED STEPS

|        | Command or Action                                                                   | Purpose                                                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal      | Enters global configuration mode.                                                                                                                                                                           |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# ip vrf vpn1 | Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode. <ul style="list-style-type: none"> <li>• The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul> |

|         | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <pre>rd route-distinguisher</pre> <p><b>Example:</b><br/>Router(config-vrf)# rd 100:1</p>                                                            | <p>Creates routing and forwarding tables.</p> <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats: <ul style="list-style-type: none"> <li>16-bit AS number: your 32-bit number, for example, 101:3</li> <li>32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul>                                                                                                                                                                                                                    |
| Step 5  | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf)# route-target import 100:1</p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |
| Step 6  | <pre>import map route-map</pre> <p><b>Example:</b><br/>Router(config-vrf)# import map vpn1-route-map</p>                                             | <p>(Optional) Configures an import route map for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-vrf)# exit</p>                                                                                  | <p>(Optional) Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 8  | <pre>interface type number</pre> <p><b>Example:</b><br/>Router(config)# interface Ethernet5/0</p>                                                    | <p>Specifies the interface to configure.</p> <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 9  | <pre>ip vrf forwarding vrf-name</pre> <p><b>Example:</b><br/>Router(config-if)# ip vrf forwarding vpn1</p>                                           | <p>Associates a VRF with the specified interface or subinterface.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 10 | <pre>end</pre> <p>Router(config-if)# end</p>                                                                                                         | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Troubleshooting Tips

Enter a **show ip vrf detail** command and make sure the MPLS VPN is up and associated with the right interfaces.

## Additional Information

For a configuration example for this task, see the [“Configuring VRFs for CSC-PE Routers: Example” section on page 37.](#)

## Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier

Perform this task to configure Multiprotocol BGP (MP-BGP) connectivity in the backbone carrier.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type*
7. **address-family vpv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community** **extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

### DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100 | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |

|         | Command or Action                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <p><b>no bgp default ipv4-unicast</b></p> <p><b>Example:</b><br/>Router(config-router)# no bgp default<br/>ipv4-unicast</p>                                                                                           | <p>(Optional) Disables the IPv4 unicast address family on all neighbors.</p> <ul style="list-style-type: none"> <li>Use the <b>no</b> form of the <b>bgp default-unicast</b> command if you are using this neighbor for MPLS routes only.</li> </ul>                                                                                                                                                               |
| Step 5  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>remote-as</b> <i>as-number</i></p> <p><b>Example:</b><br/>Router(config-router)# neighbor aa.aa.aa.aa<br/>remote-as 100</p>                    | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                         |
| Step 6  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>update-source</b> <i>interface-type</i></p> <p><b>Example:</b><br/>Router(config-router)# neighbor bb.bb.bb.bb<br/>update-source loopback0</p> | <p>Allows BGP sessions to use a specific operational interface for TCP connections.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument specifies the interface to be used as the source.</li> </ul> |
| Step 7  | <p><b>address-family vpnv4</b> [<b>unicast</b>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family vpnv4</p>                                                                                            | <p>Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.</p> <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                           |
| Step 8  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>send-community</b> <b>extended</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1<br/>send-community extended</p>      | <p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                       |
| Step 9  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor aa.aa.aa.aa<br/>activate</p>                                        | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                          |
| Step 10 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                                                                            | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                   |

## Troubleshooting Tips

You can enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. If this command is not successful, enter a **debug ip bgp x.x.x.x events** command, where *x.x.x.x* is the IP address of the neighbor.

## Additional Information

For a configuration example for this task, see the [“Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier: Example”](#) section on page 37.

## Configuring the CSC-PE and CSC-CE Routers

Perform the following tasks to configure and verify links between a CSC-PE router and the carrier CSC-CE router for an MPLS VPN CSC network that uses BGP to distribute routes and MPLS labels.

- [Configuring CSC-PE Routers, page 13](#) (required)
- [Configuring CSC-CE Routers, page 15](#) (required)
- [Verifying Labels in the CSC-PE Routers, page 17](#) (optional)
- [Verifying Labels in the CSC-CE Routers, page 20](#) (optional)

Figure 3 shows the configuration for the peering with directly connected interfaces between CSC-PE and CSC-CE routers. This configuration is used as the example in the tasks that follow.

**Figure 3** Configuration for Peering with Directly Connected Interfaces Between CSC-PE and CSC-CE Routers



## Configuring CSC-PE Routers

Perform this task to configure the CSC-PE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** *ip-address* **as-override**
8. **neighbor** *ip-address* **send-label**
9. **exit-address-family**
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                                | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                           |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn1                | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor pp.0.0.1<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                |
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor pp.0.0.1<br>activate                        | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                                 |

|         | Command or Action                                                                                                                      | Purpose                                                                                                                                                                                                                                                                             |
|---------|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>neighbor</b> <i>ip-address</i> <b>as-override</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor pp.0.0.1 as-override | Configures a PE router to override the autonomous system number (ASN) of a site with the ASN of a provider. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the router that is to be overridden with the ASN provided.</li> </ul> |
| Step 8  | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor pp.0.0.1 send-label   | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                          |
| Step 9  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                     | Exits address family configuration mode.                                                                                                                                                                                                                                            |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                        | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                           |

### Troubleshooting Tips

Enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. Make sure you see the following line in the command output under Neighbor capabilities:

```
IPv4 MPLS Label capability:advertised and received
```

### Additional Information

For a configuration example for this task, see the “[Configuring the CSC-PE Routers: Examples](#)” section on page 38.

## Configuring CSC-CE Routers

Perform this task to configure the CSC-CE routers.

### SUMMARY STEPS

- enable**
- configure terminal**
- router bgp** *as-number*
- address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
- redistribute** *protocol*
- neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
- neighbor** {*ip-address* | *peer-group-name*} **activate**
- neighbor** *ip-address* **send-label**
- exit-address-family**

## 10. end

## DETAILED STEPS

|        | Command or Action                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                        | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <b>redistribute</b> <i>protocol</i><br><br><b>Example:</b><br>Router(config-router-af)# redistribute static                                                        | Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b>, <b>egp</b>, <b>igrp</b>, <b>isis</b>, <b>ospf</b>, <b>mobile</b>, <b>static</b> [<b>ip</b>], <b>connected</b>, and <b>rip</b>. <ul style="list-style-type: none"> <li>The <b>static</b> [<b>ip</b>] keyword redistributes IP static routes. The optional <b>ip</b> keyword is used when you redistribute static routes into IS-IS.</li> <li>The <b>connected</b> keyword refers to routes which are established automatically when IP is enabled on an interface. For routing protocols such as OSPF and IS-IS, these routes are redistributed as external to the autonomous system.</li> </ul> </li> </ul> |

|         | Command or Action                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <pre><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>remote-as</b> <i>as-number</i></pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.2<br/>remote-as 100</p> | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 7  | <pre><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>activate</b></pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.2<br/>activate</p>                        | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 8  | <pre><b>neighbor</b> <i>ip-address</i> <b>send-label</b></pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.2<br/>send-label</p>                                               | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                          |
| Step 9  | <pre><b>exit-address-family</b></pre> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                                                     | <p>Exits from the address family configuration mode.</p>                                                                                                                                                                                                                                                                                                                                   |
| Step 10 | <pre><b>end</b></pre> <p><b>Example:</b><br/>Router(config-router)# end</p>                                                                                                                        | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                           |

### Additional Information

For a configuration example for this task, see the [“Configuring the CSC-CE Routers: Examples”](#) section on page 39.

## Verifying Labels in the CSC-PE Routers

Perform this task to verify the labels in the CSC-PE routers.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**summary**] [**labels**]
3. **show mpls interfaces** [**all**]
4. **show ip route vrf** *vrf-name* [*prefix*]
5. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**summary**] [**labels**]

6. **show ip cef** [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
7. **show mpls forwarding-table** [**vrf** *vrf-name*] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
8. **traceroute vrf** [*vrf-name*] *ip-address*
9. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| Step 2 | <b>show ip bgp vpnv4</b> { <b>all</b>   <b>rd</b> <i>route-distinguisher</i>   <b>vrf</b> <i>vrf-name</i> } [ <b>summary</b> ] [ <b>labels</b> ] | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>• Use the <b>show ip bgp vpnv4 all summary</b> command to check that the BGP session is up and running between the CSC-PE routers and the CSC-CE routers. Check the data in the State/PfxRcd column to verify that prefixes are learned during each session.</li> </ul>                                                                                                        |
| Step 3 | <b>show mpls interfaces</b> [ <b>all</b> ]                                                                                                       | (Optional) Displays information about one or more interfaces that have been configured for label switching. <ul style="list-style-type: none"> <li>• Use the <b>show mpls interfaces all</b> command to check that MPLS interfaces are up and running, and that LDP-enabled interfaces show that LDP is up and running. Check that LDP is turned off on the VRF because EBGp distributes the labels.</li> </ul>                                                                       |
| Step 4 | <b>show ip route vrf</b> <i>vrf-name</i> [ <i>prefix</i> ]                                                                                       | (Optional) Displays the IP routing table associated with a VRF. <ul style="list-style-type: none"> <li>• Use the <b>show ip route vrf</b> command to check that the prefixes for the PE routers are in the routing table of the CSC-PE routers.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes for the same destination learned from the CSC-CE are installed in the corresponding VRF routing table.</p> |

| Command or Action                                                                                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 5</b></p> <pre>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</pre> <p><b>Example:</b></p> <pre>Router# show ip bgp vpnv4 vrf vpn1 labels</pre>                                                                                                                                                                                 | <p>(Optional) Displays VPN address information from the BGP table.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip bgp vpnv4 vrf vrf-name labels</b> command to check that the prefixes for the customer carrier MPLS service provider networks are in the BGP table and have the appropriate labels.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the labels for the same destination learned from the CSC-CE are installed in the corresponding VRF routing table.</p>                                                    |
| <p><b>Step 6</b></p> <pre>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</pre> <p><b>Example:</b></p> <pre>Router# show ip cef vrf vpn1 aa.aa.aa.aa</pre> <pre>Router# show ip cef vrf vpn1 aa.aa.aa.aa detail</pre>                                                                                                                                   | <p>(Optional) Displays entries in the forwarding information base (FIB) or displays a summary of the FIB.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip cef vrf</b> and the <b>show ip cef vrf detail</b> commands to check that the prefixes of the PE routers are in the CEF table.</li> </ul>                                                                                                                                                                                                                                                                                    |
| <p><b>Step 7</b></p> <pre>show mpls forwarding-table [vrf vrf-name] [{{network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel [tunnel-id}}] [detail]</pre> <p><b>Example:</b></p> <pre>Router# show mpls forwarding-table vrf vpn1 aa.aa.aa.aa</pre> <pre>Router# show mpls forwarding-table vrf vpn1 aa.aa.aa.aa detail</pre> | <p>(Optional) Displays the contents of the MPLS forwarding information base (LFIB).</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command with the <b>vrf</b> keyword and both the <b>vrf</b> and <b>detail</b> keywords to check that the prefixes for the PE routers in the local customer MPLS VPN service provider are in the LFIB.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the labels for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p> |

| Command or Action                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 8</b></p> <pre>traceroute vrf [vrf-name] ip-address</pre> <p><b>Example:</b><br/>Router# traceroute vrf vpn2 jj.jj.jj.jj</p> | <p>Shows the routes that packets follow traveling through a network to their destination.</p> <ul style="list-style-type: none"> <li>Use the <b>traceroute vrf</b> command to check the data path and transport labels from a PE to a destination CE router.</li> </ul> <p><b>Note</b> This command works with MPLS-aware traceroute only if the backbone routers are configured to propagate and generate IP Time to Live (TTL) information. For more information, see the documentation on the <b>mpls ip propagate-ttl</b> command.</p> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p> |
| <p><b>Step 9</b></p> <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                      | <p>(Optional) Exits to user EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

### Additional Information

For a configuration example for this task, see the [“Verifying Labels in the CSC-PE Routers: Examples” section on page 40.](#)

## Verifying Labels in the CSC-CE Routers

Perform this task to verify the labels in the CSC-CE routers.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp summary**
3. **show ip route [address]**
4. **show mpls ldp bindings [network {mask | length}]**
5. **show ip cef [network [mask]] [longer-prefixes] [detail]**
6. **show mpls forwarding-table [vrf vrf-name] [{network {mask | length} | labels label [- label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]] [detail]**
7. **show ip bgp labels**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 2 | <p><b>show ip bgp summary</b></p> <p><b>Example:</b><br/>Router# show ip bgp summary</p>                                                                                         | <p>(Optional) Displays the status of all BGP connections.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip bgp summary</b> command to check that the BGP session is up and running on the CSC-CE routers.</li> </ul>                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <p><b>show ip route</b> [address]</p> <p><b>Example:</b><br/>Router# show ip route aa.aa.aa.aa</p>                                                                               | <p>(Optional) Displays IP routing table entries.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> command to check that the loopback address of the local and remote PE routers are in the routing table.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p>                                                                                     |
| Step 4 | <p><b>show mpls ldp bindings</b> [network {mask   length}]</p> <p><b>Example:</b><br/>Router# show mpls ldp bindings aa.aa.aa.aa 255.255.255.255</p>                             | <p>(Optional) Displays the contents of the label information base (LIB).</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp bindings</b> command to check that the prefix of the local PE router is in the MPLS LDP bindings.</li> </ul>                                                                                                                                                                                                                                                                                          |
| Step 5 | <p><b>show ip cef</b> [network [mask]] [longer-prefixes] [detail]</p> <p><b>Example:</b><br/>Router# show ip cef aa.aa.aa.aa<br/><br/>Router# show ip cef aa.aa.aa.aa detail</p> | <p>(Optional) Displays entries in the forwarding information base (FIB) or a summary of the FIB.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> and the <b>show ip cef detail</b> commands to check that the prefixes of the local and remote PE routers are in the CEF table.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes and the labels for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p> |

| Command or Action                                                                                                                                                                                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 6</b></p> <pre>show mpls forwarding-table [vrf vrf-name] [<i>{network {mask   length}   labels label</i> [<i>- label</i>]   <i>interface interface   next-hop</i> <i>address   lsp-tunnel [tunnel-id]</i>] [<i>detail</i>]</pre> <p><b>Example:</b></p> <pre>Router# show mpls forwarding-table aa.aa.aa.aa</pre> <pre>Router# show mpls forwarding-table aa.aa.aa.aa detail</pre> | <p>(Optional) Displays the contents of the MPLS LFIB.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> and <b>show mpls forwarding-table detail</b> commands to check that the prefixes of the local and remote PE routers are in the MPLS forwarding table.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes and labels for the same destination learned from the CSC-CE are installed in the corresponding VRF routing table.</p> |
| <p><b>Step 7</b></p> <pre>show ip bgp labels</pre> <p><b>Example:</b></p> <pre>Router# show ip bgp labels</pre>                                                                                                                                                                                                                                                                               | <p>(Optional) Displays information about MPLS labels from the EBGp route table.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip bgp labels</b> command to check that the BGP routing table contains labels for prefixes in the customer carrier MPLS VPN service provider networks.</li> </ul>                                                                                                                                                                                                                                      |

### Additional Information

For a configuration example for this task, see the [“Verifying Labels in the CSC-CE Routers: Examples” section on page 43](#).

## Configuring the Customer Carrier Network

Perform the following tasks to configure and verify the customer carrier network. This requires setting up connectivity and routing functions for the customer carrier core (P) routers and the customer carrier edge (PE) routers.

- [Verifying IP Connectivity in the Customer Carrier, page 23](#) (optional)
- [Configuring a Customer Carrier Core Router as a Route Reflector, page 24](#) (optional)

### Prerequisites

Before you configure an MPLS VPN CSC network that uses BGP to distribute routes and MPLS labels, you must configure the following on your customer carrier routers:

- An IGP routing protocol—BGP, OSPF, IS-IS, EIGRP, static, and so on. For information, see the “IP Routing Protocols” chapter in the [Cisco IOS IP Configuration Guide, Release 12.0](#).
- MPLS VPN functionality on the PE routers (for hierarchical VPNs only). For information, see the [MPLS Virtual Private Networks \(VPNs\)](#) or the [MPLS Virtual Private Network Enhancements](#).
- Label Distribution Protocol (LDP) on P and PE routers (for hierarchical VPNs only). For information, see the [MPLS Label Distribution Protocol \(LDP\)](#).



#### Note

You must configure the items in the preceding list before performing the tasks in this section.

## Verifying IP Connectivity in the Customer Carrier

Perform this task to verify IP connectivity in the customer carrier.

### SUMMARY STEPS

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route**
5. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                          |
| Step 2 | <b>ping</b> [ <i>protocol</i> ] { <i>host-name</i>   <i>system-address</i> }<br><br><b>Example:</b><br>Router# ping ip <P-address> | Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks. <ul style="list-style-type: none"> <li>• Use the <b>ping</b> command to verify the connectivity from one customer carrier core router to another.</li> </ul>                                                                                   |
| Step 3 | <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ]<br><br><b>Example:</b><br>Router# trace ip destination-address             | Discovers the routes that packets will actually take when traveling to their destination. <ul style="list-style-type: none"> <li>• Use the <b>trace</b> command to verify the path that a packet goes through before reaching the final destination. The <b>trace</b> command can help isolate a trouble spot if two routers cannot communicate.</li> </ul> |
| Step 4 | <b>show ip route</b><br><br><b>Example:</b><br>Router# show ip route                                                               | Displays IP routing table entries. <ul style="list-style-type: none"> <li>• Use the <b>show ip route</b> command to display the entire routing table, including host IP address, next hop, interface, and so forth.</li> </ul>                                                                                                                              |
| Step 5 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                           | Returns to user mode.                                                                                                                                                                                                                                                                                                                                       |

### Additional Information

For a configuration example for this task, see the [“Verifying IP Connectivity in the Customer Carrier: Example”](#) section on page 45.

## Configuring a Customer Carrier Core Router as a Route Reflector

Perform this task to configure a customer carrier core (P) router as a route reflector of multiprotocol BGP prefixes.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family vpnv4** [unicast]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** *ip-address* **route-reflector-client**
8. **exit-address-family**
9. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                             | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and labels the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.1.1.1<br>remote-as 100 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>• The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>• The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>• The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                    |

|        | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>address-family vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                    | Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                  |
| Step 6 | <b>neighbor {ip-address   peer-group-name} activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.1.1.1 activate         | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 7 | <b>neighbor ip-address route-reflector-client</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.1.1.1 route-reflector-client | Configures the router as a BGP route reflector and configures the specified neighbor as its client. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP neighbor being identified as a client.</li> </ul>                    |
| Step 8 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                             | Exits address family configuration mode.                                                                                                                                                                                                                                           |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                          |

### Troubleshooting Tips

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. For neighbors to exchange other address prefix types, such as multicast and VPNv4, you must also activate neighbors using the **neighbor activate** command in address family configuration mode, as shown.

Route reflectors and clients (neighbors or internal BGP peer groups) that are defined in router configuration mode using the **neighbor route-reflector-client** command reflect unicast address prefixes to and from those clients by default. To cause them to reflect prefixes for other address families, such as multicast, define the reflectors and clients in address family configuration mode, using the **neighbor route-reflector-client** command, as shown.

### Additional Information

For a configuration example for this task, see the [“Configuring a Customer Carrier Core Router as a Route Reflector: Example”](#) section on page 46.

## Configuring the Customer Site for Hierarchical VPNs

**Note**

This section applies only to customer carrier networks that use BGP to distribute routes and MPLS labels.

Perform the following tasks to configure and verify the customer site for hierarchical VPNs:

- [Defining VPNs on PE Routers for Hierarchical VPNs, page 26](#) (required)
- [Configuring BGP Routing Sessions on the PE Routers for Hierarchical VPNs, page 27](#) (required)
- [Verifying Labels in Each PE Router for Hierarchical VPNs, page 29](#) (optional)
- [Configuring CE Routers for Hierarchical VPNs, page 30](#) (required)
- [Verifying IP Connectivity in the Customer Site, page 33](#) (optional)

**Note**

This section applies to hierarchical VPNs only.

## Defining VPNs on PE Routers for Hierarchical VPNs

Perform this task to define VPNs on PE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf *vrf-name***
4. **rd *route-distinguisher***
5. **route-target {import | export | both} *route-target-ext-community***
6. **import map *route-map***
7. **ip vrf forwarding *vrf-name***
8. **exit**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|        | Command or Action                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>ip vrf vrf-name</pre> <p><b>Example:</b><br/>Router(config)# ip vrf vpn2 </p>                                                                    | <p>Creates a VRF routing table and a CEF forwarding table and enters VRF configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is a name you assign to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | <pre>rd route-distinguisher</pre> <p><b>Example:</b><br/>Router(config-vrf)# rd 200:1 </p>                                                            | <p>Creates routing and forwarding tables for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 5 | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf)# route-target export 200:1 </p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and export routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |
| Step 6 | <pre>import map route-map</pre> <p><b>Example:</b><br/>Router(config-vrf)# import map map23 </p>                                                      | <p>Configures an import route map for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 7 | <pre>ip vrf forwarding vrf-name</pre> <p><b>Example:</b><br/>Router(config-vrf)# ip vrf forwarding vpn2 </p>                                          | <p>Associates a VPN VRF instance with an interface or subinterface.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-vrf)# exit </p>                                                                                  | <p>Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

### Additional Information

For a configuration example for this task, see the “[Configuring PE Routers for Hierarchical VPNs: Examples](#)” section on page 46.

## Configuring BGP Routing Sessions on the PE Routers for Hierarchical VPNs

Perform this task to configure BGP routing sessions on the PE routers for PE-to-CE router communication.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                               | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                  | Configures the router to run a BGP process and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                     |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 multicast | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>• The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>• The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>• The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |

|        | Command or Action                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>neighbor {ip-address   peer-group-name} remote-as as-number</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor aa.aa.aa.aa<br/>remote-as 300</p> | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 6 | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor bb.bb.bb.bb<br/>activate</p>                 | <p>Enables the exchange of information with a neighboring router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                      |
| Step 7 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                            | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                           |

### Additional Information

For a configuration example for this task, see the [“Configuring PE Routers for Hierarchical VPNs: Examples” section on page 46](#).

## Verifying Labels in Each PE Router for Hierarchical VPNs

Perform this task to verify labels in each PE router for hierarchical VPNs.

### SUMMARY STEPS

1. **enable**
2. **show ip route vrf** *vrf-name* [*prefix*]
3. **show mpls forwarding-table** [**vrf** *vrf-name*] [*prefix*] [**detail**]
4. **show ip cef** [*network* [*mask* [**longer-prefix**]]] [**detail**]
5. **show ip cef vrf** *vrf-name* [*ip-prefix*]
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                              |
| Step 2 | <b>show ip route vrf</b> <i>vrf-name</i> [ <i>prefix</i> ]<br><br><b>Example:</b><br>Router# show ip route vrf vpn2 aa.aa.aa.aa                                                                                                                       | (Optional) Displays the IP routing table associated with a VRF. <ul style="list-style-type: none"> <li>Use the <b>show ip route vrf</b> command to check that the loopback addresses of the local and remote CE routers are in the routing table of the PE routers.</li> </ul>                |
| Step 3 | <b>show mpls forwarding-table</b> [ <i>vrf vrf-name</i> ] [ <i>prefix</i> ] [ <i>detail</i> ]<br><br><b>Example:</b><br>Router# show mpls forwarding-table vrf vpn2 aa.aa.aa.aa<br><br>Router# show mpls forwarding-table vrf vpn2 aa.aa.aa.aa detail | (Optional) Displays the contents of the LFIB. <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command to check that the prefixes for the local and remote CE routers are in the MPLS forwarding table, and that the specified prefix is untagged.</li> </ul> |
| Step 4 | <b>show ip cef</b> [ <i>network</i> [ <i>mask</i> [ <i>longer-prefix</i> ]]] [ <i>detail</i> ]<br><br><b>Example:</b><br>Router# show ip cef aa.aa.aa.aa<br><br>Router# show ip cef aa.aa.aa.aa detail                                                | (Optional) Displays specific entries in the FIB based on IP address information. <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> command to check that the prefixes of the local and remote PE routers are in the CEF table.</li> </ul>                                     |
| Step 5 | <b>show ip cef vrf</b> <i>vrf-name</i> [ <i>ip-prefix</i> ]<br><br><b>Example:</b><br>Router# show ip cef vrf vpn2 aa.aa.aa.aa                                                                                                                        | (Optional) Displays the CEF forwarding table associated with a VRF. <ul style="list-style-type: none"> <li>Use the <b>show ip cef vrf</b> command to check that the prefix of the remote CE router is in the CEF table.</li> </ul>                                                            |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                                                                                    | (Optional) Exits to user EXEC mode.                                                                                                                                                                                                                                                           |

## Additional Information

For a configuration example for this task, see the [“Verifying Labels in Each PE Router for Hierarchical VPNs: Examples”](#) section on page 47.

## Configuring CE Routers for Hierarchical VPNs

Perform this task to configure CE routers for hierarchical VPNs. This configuration is the same as that for an MPLS VPN that is not in a hierarchical topology.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **interface** *type number*
5. **ip address** *ip-address mask* [**secondary**]
6. **exit**
7. **router bgp** *as-number*
8. **redistribute** *protocol*
9. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>ip cef [distributed]</b><br><br><b>Example:</b><br>Router(config)# ip cef distributed           | Enables CEF on the route processor card. <ul style="list-style-type: none"> <li>• The <b>distributed</b> keyword enables distributed CEF (dCEF) operation. CEF information is distributed to the line cards. Line cards perform express forwarding.</li> </ul>                                                                                                                                                                                                                                                                                                                                                    |
| Step 4 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 0 | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type</i> argument specifies the type of interface to be configured. <ul style="list-style-type: none"> <li>– A loopback interface indicates a software-only interface that emulates an interface that is always up. It is a virtual interface supported on all platforms.</li> </ul> </li> <li>• The <i>number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.</li> </ul> |

|         | Command or Action                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <p><b>ip address</b> <i>ip-address mask [secondary]</i></p> <p><b>Example:</b><br/> Router(config-if)# ip address aa.aa.aa.aa<br/> 255.255.2355.255</p>                                                 | <p>Sets a primary or secondary IP address for an interface.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul>                                                                                                                                                                                                                                                           |
| Step 6  | <p><b>exit</b></p> <p><b>Example:</b><br/> Router(config-if)# exit</p>                                                                                                                                  | <p>Exits interface configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 7  | <p><b>router bgp</b> <i>as-number</i></p> <p><b>Example:</b><br/> Router(config)# router bgp 100</p>                                                                                                    | <p>Configures a BGP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                                                                                                                                                                |
| Step 8  | <p><b>redistribute</b> <i>protocol</i></p> <p><b>Example:</b><br/> Router(config-router)# redistribute connected</p>                                                                                    | <p>Redistributes routes from one routing domain into another routing domain.</p> <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b>, <b>connected</b>, <b>egp</b>, <b>igrp</b>, <b>isis</b>, <b>mobile</b>, <b>ospf</b>, <b>static [ip]</b>, or <b>rip</b>.</li> </ul> <p>The <b>connected</b> keyword refers to routes that are established automatically when IP is enabled on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes are redistributed as external to the autonomous system.</p> |
| Step 9  | <p><b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br/> <b>remote-as</b> <i>as-number</i></p> <p><b>Example:</b><br/> Router(config-router)# neighbor aa.aa.aa.aa<br/> remote-as 100</p> | <p>Adds the IP address of the neighbor in the remote autonomous system to the multiprotocol BGP neighbor table of the local router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                                                                                                  |
| Step 10 | <p><b>end</b></p> <p><b>Example:</b><br/> Router(config-router)# end</p>                                                                                                                                | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Additional Information

For a configuration example for this task, see the “Configuring CE Routers for Hierarchical VPNs: Examples” section on page 48.

## Verifying IP Connectivity in the Customer Site

Perform this task to verify IP connectivity in the customer site.

### SUMMARY STEPS

1. **enable**
2. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** {*access-list-number* | *access-list-name*}]
3. **ping** [*protocol*] {*host-name* | *system-address*}
4. **trace** [*protocol*] [*destination*]
5. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                   |
| Step 2 | <b>show ip route</b> [ <i>ip-address</i> [ <i>mask</i> ] [ <b>longer-prefixes</b> ]]   [ <i>protocol</i> [ <i>process-id</i> ]]   [ <b>list</b> { <i>access-list-number</i>   <i>access-list-name</i> }]<br><br><b>Example:</b><br>Router# show ip route bb.bb.bb.bb | (Optional) Displays the current state of the routing table. <ul style="list-style-type: none"> <li>• Use the <b>show ip route</b> <i>ip-address</i> command to check that the loopback addresses of the remote CE routers learned through the PE router are in the routing table of the local CE routers.</li> </ul> |
| Step 3 | <b>ping</b> [ <i>protocol</i> ] { <i>host-name</i>   <i>system-address</i> }<br><br><b>Example:</b><br>Router# ping bb.bb.bb.bb                                                                                                                                      | Diagnoses basic network connectivity on Apollo, AppleTalk, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, VINES, or XNS networks. <ul style="list-style-type: none"> <li>• Use the <b>ping</b> command to check connectivity between customer site routers.</li> </ul>                               |

|        | Command or Action                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <pre>trace [protocol] [destination]</pre> <p><b>Example:</b><br/>Router# trace ip bb.bb.bb.bb</p> | <p>Discovers the routes that packets will actually take when traveling to their destination.</p> <ul style="list-style-type: none"> <li>Use the <b>trace</b> command to follow the path of the packets in the customer site.</li> <li>To use nondefault parameters and invoke an extended <b>trace test</b>, enter the <b>trace</b> command without a destination argument. You will be stepped through a dialog to select the desired parameters.</li> </ul> |
| Step 5 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                     | (Optional) Exits to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Additional Information

For a configuration example for this task, see the “[Verifying IP Connectivity in the Customer Site: Examples](#)” section on page 49.

## Configuration Examples for MPLS VPN CSC with BGP

Configuration examples for the MPLS VPN CSC with BGP include the following:

- [Configuring the Backbone Carrier Core: Examples, page 35](#)
- [Configuring the Links Between CSC-PE and CSC-CE Routers: Examples, page 38](#)
- [Configuring the Customer Carrier Network: Examples, page 45](#)
- [Configuring the Customer Site for Hierarchical VPNs: Examples, page 46](#)

Figure 4 shows a sample CSC topology for exchanging IPv4 routes and MPLS labels. Use this figure as a reference for configuring and verifying carrier supporting carrier routers to exchange IPv4 routes and MPLS labels.

**Figure 4** Sample CSC Topology for Exchanging IPv4 Routes and MPLS Labels

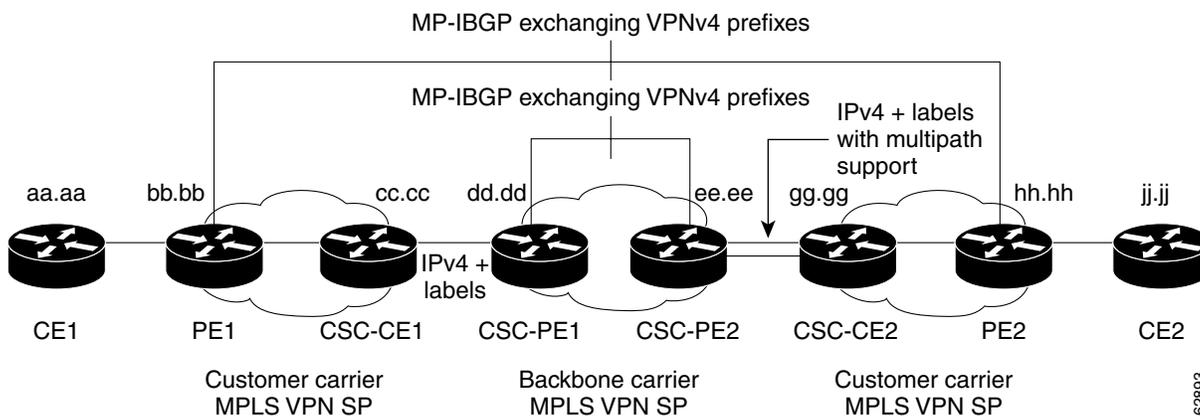


Table 1 describes the sample configuration shown in Figure 4.

**Table 1** Description of Sample Configuration Shown in [Figure 4](#)

| Routers             | Description                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CE1 and CE2         | <p>Belong to an end customer. CE1 and CE2 routers exchange routes learned from PE routers.</p> <p>The end customer is purchasing VPN services from a customer carrier.</p>                                                                                                                                                                                            |
| PE1 and PE2         | <p>Part of a customer carrier network that is configured to provide MPLS VPN services. PE1 and PE2 are peering with a VPNv4 IBGP session to form an MPLS VPN network.</p>                                                                                                                                                                                             |
| CSC-CE1 and CSC-CE2 | <p>Part of a customer carrier network. CSC-CE1 and CSC-CE2 routers exchange IPv4 BGP updates with MPLS labels and redistribute PE loopback addressees to and from the IGP (OSPF in this example).</p> <p>The customer carrier is purchasing carrier supporting carrier VPN services from a backbone carrier.</p>                                                      |
| CSC-PE1 and CSC-PE2 | <p>Part of the backbone carrier's network configured to provide carrier supporting carrier VPN services. CSC-PE1 and CSC-PE2 are peering with a VPNv4 IP BGP session to form the MPLS VPN network. In the VRF, CSC-PE1 and CSC-PE2 are peering with the CSC-CE routers, which are configured for carrying MPLS labels with the routes, with an IPv4 EBGP session.</p> |

## Configuring the Backbone Carrier Core: Examples

Configuration and verification examples for the backbone carrier core included in this section are as follows:

- [Verifying IP Connectivity and LDP Configuration in the CSC Core: Example, page 35](#)
- [Configuring VRFs for CSC-PE Routers: Example, page 37](#)
- [Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier: Example, page 37](#)

### Verifying IP Connectivity and LDP Configuration in the CSC Core: Example

Check that CSC-PE2 is reachable from CSC-PE1 by entering the following command on CSC-CE1:

```
Router# ping ee.ee.ee.ee
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to ee.ee.ee.ee, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

Verify the path from CSC-PE1 to CSC-PE2 by entering the following command on CSC-CE1:

```
Router# trace ee.ee.ee.ee
```

```
Type escape sequence to abort.
```

```
Tracing the route to ee.ee.ee.ee
```

```
 1 ee.ee.ee.ee 0 msec 0 msec *
```

Check that CSC-PE router prefixes are in the MPLS forwarding table:

```
Router# show mpls forwarding-table
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|-----------|--------------------|---------------------|--------------------|--------------------|-------------|
| 16        | 2/nn               | dd.dd.dd.dd/32      | 0                  | AT2/1/0.1          | point2point |
| 17        | 16                 | bb.bb.bb.bb/32 [V]  | 30204              | Et1/0              | pp.0.0.1    |
| 21        | Pop tag            | cc.cc.cc.cc/32 [V]  | 0                  | Et1/0              | pp.0.0.1    |
| 22        | Pop tag            | nn.0.0.0/8 [V]      | 570                | Et1/0              | pp.0.0.1    |
| 23        | Aggregate          | pp.0.0.0/8 [V]      | 0                  |                    |             |
| 2         | 2/nn               | gg.gg.gg.gg/32 [V]  | 0                  | AT3/0.1            | point2point |
| 8         | 2/nn               | hh.hh.hh.hh/32 [V]  | 15452              | AT3/0.1            | point2point |
| 29        | 2/nn               | qq.0.0.0/8 [V]      | 0                  | AT3/0.1            | point2point |
| 30        | 2/nn               | ss.0.0.0/8 [V]      | 0                  | AT3/0.1            | point2point |

Check the status of LDP discovery processes in the core:

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
ee.ee.ee.ee:0
Discovery Sources:
Interfaces:
 ATM2/1/0.1 (ldp): xmit/rcv
 TDP Id: dd.dd.dd.dd:1
```

Check the status of LDP sessions in the core:

```
Router# show mpls ldp neighbor
```

```
Peer LDP Ident: dd.dd.dd.dd:1; Local LDP Ident ee.ee.ee.ee:1
TCP connection: dd.dd.dd.dd.646 - ee.ee.ee.ee.11007
State: Oper; Msgs sent/rcvd: 20/21; Downstream on demand
Up time: 00:14:56
LDP discovery sources:
 ATM2/1/0.1, Src IP addr: dd.dd.dd.dd
```

Check the forwarding table (prefixes, next-hops, and interfaces):

```
Router# show ip cef
```

| Prefix             | Next Hop    | Interface                           |
|--------------------|-------------|-------------------------------------|
| 0.0.0.0/0          | drop        | Null0 (default route handler entry) |
| 0.0.0.0/32         | receive     |                                     |
| dd.dd.dd.dd/32     | dd.dd.dd.dd | ATM2/1/0.1                          |
| ee.ee.ee.ee/32     | receive     |                                     |
| 224.0.0.0/4        | drop        |                                     |
| 224.0.0.0/24       | receive     |                                     |
| 255.255.255.255/32 | receive     |                                     |



#### Note

Also see the [“Verifying Labels in the CSC-CE Routers: Examples”](#) section on page 43.

Verify that interfaces are configured to use LDP:

```
Router# show mpls interfaces
```

| Interface   | IP        | Tunnel | Operational |
|-------------|-----------|--------|-------------|
| Ethernet0/1 | Yes (ldp) | No     | Yes         |

Display the entire routing table, including host IP address, next hop, interface, and so forth:

```
Router# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set

 dd.0.0.0/32 is subnetted, 1 subnets
O dd.dd.dd.dd [110/7] via dd.dd.dd.dd, 00:16:42, ATM2/1/0.1
 ee.0.0.0/32 is subnetted, 1 subnets
C ee.ee.ee.ee is directly connected, Loopback0
```

## Configuring VRFs for CSC-PE Routers: Example

The following example shows how to configure a VPN routing/forwarding instance (VRF) for a CSC-PE router:

```
ip cef distributed

ip vrf vpn1
rd 100:1
route target both 100:1
!
```

## Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier: Example

The following example shows how to configure Multiprotocol BGP (MP-BGP) for VPN connectivity in the backbone carrier:

```
ip cef distributed

ip vrf vpn1
rd 100:1
route target both 100:1

hostname csc-pe1
!
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor ee.ee.ee.ee remote-as 100
 neighbor ee.ee.ee.ee update-source Loopback0
 no auto-summary
!
 address-family vpnv4
 neighbor ee.ee.ee.ee activate
 neighbor ee.ee.ee.ee send-community extended
 bgp dampening 30
 exit-address-family
!
router bgp 100
. . .
! (BGP IPv4 to CSC-CE router from CSC-PE router)
!
```

```

address-family ipv4 vrf vpn1
neighbor ss.0.0.2 remote-as 200
neighbor ss.0.0.2 activate
neighbor ss.0.0.2 as-override
neighbor ss.0.0.2 advertisement-interval 5
neighbor ss.0.0.2 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family
!
```

## Configuring the Links Between CSC-PE and CSC-CE Routers: Examples

This section contains the following examples:

- [Configuring the CSC-PE Routers: Examples, page 38](#)
- [Configuring the CSC-CE Routers: Examples, page 39](#)
- [Verifying Labels in the CSC-PE Routers: Examples, page 40](#)
- [Verifying Labels in the CSC-CE Routers: Examples, page 43](#)

## Configuring the CSC-PE Routers: Examples

The following example shows how to configure a CSC-PE router:

```

ip cef
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
mpls label protocol ldp
!
interface Loopback0
 ip address dd.dd.dd.dd 255.255.255.255
!
interface Ethernet3/1
 ip vrf forwarding vpn1
 ip address pp.0.0.2 255.0.0.0
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 mpls
 ip unnumbered Loopback0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
```

```

redistribute connected subnets
passive-interface Ethernet3/1
network dd.dd.dd.dd 0.0.0.0 area 100
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30
neighbor ee.ee.ee.ee remote-as 100
neighbor ee.ee.ee.ee update-source Loopback0
!
address-family vpnv4 !VPNv4 session with CSC-PE2
neighbor ee.ee.ee.ee activate
neighbor ee.ee.ee.ee send-community extended
bgp dampening 30
exit-address-family
!
address-family ipv4 vrf vpn1
neighbor pp.0.0.1 remote-as 200
neighbor pp.0.0.1 activate
neighbor pp.0.0.1 as-override
neighbor pp.0.0.1 advertisement-interval 5
neighbor pp.0.0.1 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## Configuring the CSC-CE Routers: Examples

The following example shows how to configure a CSC-CE router:

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
ip address cc.cc.cc.cc 255.255.255.255
!
interface Ethernet3/0
ip address pp.0.0.1 255.0.0.0
!
interface Ethernet4/0
ip address mn.0.0.2 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets !Exchange routes
redistribute bgp 200 metric 3 subnets !learned from PE1
passive-interface ATML1/0
passive-interface Ethernet3/0
network cc.cc.cc.cc 0.0.0.0 area 200
network mn.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30

```

```

neighbor pp.0.0.2 remote-as 100
neighbor pp.0.0.2 update-source Ethernet3/0
no auto-summary
!
address-family ipv4
 redistribute connected
 redistribute ospf 200 metric 4 match internal
 neighbor pp.0.0.2 activate
 neighbor pp.0.0.2 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## Verifying Labels in the CSC-PE Routers: Examples

The following examples show how to verify the configurations of the CSC-PE routers.

Verify that the BGP session is up and running between the CSC-PE router and the CSC-CE router. Check the data in the State/PfxRcd column to verify that prefixes are learned during each session.

```
Router# show ip bgp vpnv4 all summary
```

```

BBGP router identifier dd.dd.dd.dd, local AS number 100
BGP table version is 52, main routing table version 52
12 network entries and 13 paths using 2232 bytes of memory
6 BGP path attribute entries using 336 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 16/4 prefixes, 27/14 paths, scan interval 5 secs

```

| Neighbor    | V | AS  | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down  | State/PfxRcd |
|-------------|---|-----|---------|---------|--------|-----|------|----------|--------------|
| ee.ee.ee.ee | 4 | 100 | 7685    | 7686    | 52     | 0   | 0    | 21:17:04 | 6            |
| pp.0.0.2    | 4 | 200 | 7676    | 7678    | 52     | 0   | 0    | 21:16:43 | 7            |

Verify that the MPLS interfaces are up and running, and that LDP-enabled interfaces show that LDP is up and running. LDP is turned off on the VRF because EBGP distributes the labels.

```
Router# show mpls interfaces all
```

| Interface          | IP        | Tunnel | Operational |
|--------------------|-----------|--------|-------------|
| GigabitEthernet6/0 | Yes (ldp) | No     | Yes         |
| VRF vpn1:          |           |        |             |
| Ethernet3/1        | No        | No     | Yes         |

Verify that the prefix for the local PE router is in the routing table of the CSC-PE router:

```
Router# show ip route vrf vpn2 bb.bb.bb.bb
```

```

Routing entry for bb.bb.bb.bb/32
 Known via "bgp 100", distance 20, metric 4
 Tag 200, type external
 Last update from pp.0.0.2 21:28:39 ago
 Routing Descriptor Blocks:
 * pp.0.0.2, from pp.0.0.2, 21:28:39 ago
 Route metric is 4, traffic share count is 1
 AS Hops 1, BGP network version 0

```

Verify that the prefix for the remote PE router is in the routing table of the CSC-PE router:

```
Router# show ip route vrf vpn2 hh.hh.hh.hh

Routing entry for hh.hh.hh.hh/32
 Known via "bgp 100", distance 200, metric 4
 Tag 200, type internal
 Last update from ee.aa.aa.aa 21:27:39 ago
 Routing Descriptor Blocks:
 * ee.aa.aa.aa (Default-IP-Routing-Table), from ee.aa.aa.aa, 21:27:39 ago
 Route metric is 4, traffic share count is 1
 AS Hops 1, BGP network version 0
```

Verify that the prefixes for the customer carrier MPLS VPN service provider networks are in the BGP table, and have appropriate labels:

```
Router# show ip bgp vpnv4 vrf vpn2 labels

Network Next Hop In label/Out label
Route Distinguisher: 100:1 (vpn1)
cc.cc.cc.cc/32 pp.0.0.2 22/imp-null
bb.bb.bb.bb/32 pp.0.0.2 27/20
hh.hh.hh.hh/32 ee.aa.aa.aa 34/35
gg.gg.gg.gg/32 ee.aa.aa.aa 30/30
nn.0.0.0 pp.0.0.2 23/imp-null
ss.0.0.0 ee.aa.aa.aa 33/34
pp.0.0.0 pp.0.0.2 25/aggregate(vpn1)
```

Verify that the prefix of the PE router in the local customer carrier MPLS VPN service provider is in the CEF table:

```
Router# show ip cef vrf vpn2 bb.bb.bb.bb

bb.bb.bb.bb/32, version 19, cached adjacency pp.0.0.2
0 packets, 0 bytes
 tag information set
 local tag: 27
 fast tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
 via pp.0.0.2, 0 dependencies, recursive
 next hop pp.0.0.2, Ethernet3/1 via pp.0.0.2/32
 valid cached adjacency
 tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
```

```
Router# show ip cef vrf vpn2 bb.bb.bb.bb detail

bb.bb.bb.bb/32, version 19, cached adjacency pp.0.0.2
0 packets, 0 bytes
 tag information set
 local tag: 27
 fast tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
 via pp.0.0.2, 0 dependencies, recursive
 next hop pp.0.0.2, Ethernet3/1 via pp.0.0.2/32
 valid cached adjacency
 tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
```

Verify that the prefix of the PE router in the local customer carrier MPLS VPN service provider is in the MPLS forwarding table:

```
Router# show mpls forwarding-table vrf vpn2 bb.bb.bb.bb

Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
27 20 bb.bb.bb.bb/32[V] 958048 Et3/1 pp.0.0.2
```

```
Router# show mpls forwarding-table vrf vpn2 bb.bb.bb.bb detail

Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
27 20 bb.bb.bb.bb/32[V] 958125 Et3/1 pp.0.0.2
 MAC/Encaps=14/18, MTU=1500, Tag Stack{20}
 00B04A74A05400B0C26E10558847 00014000
 VPN route: vpn1
 No output feature configured
 Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

Verify that the prefix of the PE router in the remote customer carrier MPLS VPN service provider is in the CEF table:

```
Router# show ip cef vrf vpn2 hh.hh.hh.hh

hh.hh.hh.hh/32, version 25, cached adjacency rr.0.0.2
0 packets, 0 bytes
tag information set
 local tag: 34
 fast tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
via ee.ee.ee.ee, 0 dependencies, recursive
 next hop rr.0.0.2, GigabitEthernet6/0 via ee.ee.ee.ee/32
 valid cached adjacency
 tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
```

```
Router# show ip cef vrf vpn2 hh.hh.hh.hh detail

hh.hh.hh.hh/32, version 25, cached adjacency rr.0.0.2
0 packets, 0 bytes
tag information set
 local tag: 34
 fast tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
via ee.ee.ee.ee, 0 dependencies, recursive
 next hop rr.0.0.2, GigabitEthernet6/0 via ee.ee.ee.ee/32
 valid cached adjacency
 tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
```

Verify that the prefix of the PE router in the remote customer carrier MPLS VPN service provider is in the MPLS forwarding table:

```
Router# show mpls forwarding-table vrf vpn2 hh.hh.hh.hh

Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
34 35 hh.hh.hh.hh/32[V] 139034 Gi6/0 rr.0.0.2

Router# show mpls forwarding-table vrf vpn2 hh.hh.hh.hh detail

Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
34 35 hh.hh.hh.hh/32[V] 139034 Gi6/0 rr.0.0.2
 MAC/Encaps=14/18, MTU=1500, Tag Stack{35}
 00B0C26E447000B0C26E10A88847 00023000
 VPN route: vpn1
 No output feature configured
 Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

## Verifying Labels in the CSC-CE Routers: Examples

The following examples show how to verify the configurations of the CSC-CE routers.

Verify that the BGP session is up and running:

```
Router# show ip bgp summary
```

```
BGP router identifier cc.cc.cc.cc, local AS number 200
BGP table version is 35, main routing table version 35
14 network entries and 14 paths using 2030 bytes of memory
3 BGP path attribute entries using 168 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 1 history paths, 0 dampened paths
BGP activity 17/67 prefixes, 29/15 paths, scan interval 60 secs
```

| Neighbor | V | AS  | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down  | State/PfxRcd |
|----------|---|-----|---------|---------|--------|-----|------|----------|--------------|
| pp.0.0.1 | 4 | 100 | 7615    | 7613    | 35     | 0   | 0    | 21:06:19 | 5            |

Verify that the loopback address of the local PE router is in the routing table:

```
Router# show ip route bb.bb.bb.bb
```

```
Routing entry for bb.bb.bb.bb/32
 Known via "ospf 200", distance 110, metric 101, type intra area
 Redistributing via bgp 200
 Advertised by bgp 200 metric 4 match internal
 Last update from nn.0.0.1 on Ethernet4/0, 00:34:08 ago
 Routing Descriptor Blocks:
 * nn.0.0.1, from bb.bb.bb.bb, 00:34:08 ago, via Ethernet4/0
 Route metric is 101, traffic share count is 1
```

Verify that the loopback address of the remote PE router is in the routing table:

```
Router# show ip route hh.hh.hh.hh
```

```
Routing entry for hh.hh.hh.hh/32
 Known via "bgp 200", distance 20, metric 0
 Tag 100, type external
 Redistributing via ospf 200
 Advertised by ospf 200 metric 3 subnets
 Last update from pp.0.0.1 00:45:16 ago
 Routing Descriptor Blocks:
 * pp.0.0.1, from pp.0.0.1, 00:45:16 ago
 Route metric is 0, traffic share count is 1
 AS Hops 2, BGP network version 0
```

Verify that the prefix of the local PE router is in the MPLS LDP bindings:

```
Router# show mpls ldp bindings bb.bb.bb.bb 255.255.255.255
```

```
tib entry: bb.bb.bb.bb/32, rev 20
 local binding: tag: 20
 remote binding: tsr: bb.bb.bb.bb:0, tag: imp-null
```

Verify that the prefix of the local PE router is in the CEF table:

```
Router# show ip cef bb.bb.bb.bb
```

```
bb.bb.bb.bb/32, version 46, cached adjacency nn.0.0.1
0 packets, 0 bytes
 tag information set
 local tag: 20
```

```

via nn.0.0.1, Ethernet4/0, 0 dependencies
next hop nn.0.0.1, Ethernet4/0
unresolved
valid cached adjacency
tag rewrite with Et4/0, nn.0.0.1, tags imposed {}

```

Verify that the prefix of the local PE router is in the MPLS forwarding table:

```
Router# show mpls forwarding-table bb.bb.bb.bb
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 20        | Pop tag            | bb.bb.bb.bb/32      | 893397             | Et4/0              | nn.0.0.1 |

```
Router# show mpls forwarding-table bb.bb.bb.bb detail
```

| Local tag                                                             | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------------------------------------------------------------------|--------------------|---------------------|--------------------|--------------------|----------|
| 20                                                                    | Pop tag            | bb.bb.bb.bb/32      | 893524             | Et4/0              | nn.0.0.1 |
| MAC/Encaps=14/14, MTU=1504, Tag Stack{}                               |                    |                     |                    |                    |          |
| 00074F83685400B04A74A0708847                                          |                    |                     |                    |                    |          |
| No output feature configured                                          |                    |                     |                    |                    |          |
| Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 |                    |                     |                    |                    |          |

Verify that the BGP routing table contains labels for prefixes in the customer carrier MPLS VPN service provider networks:

```
Router# show ip bgp labels
```

| Network        | Next Hop | In Label/Out Label |
|----------------|----------|--------------------|
| cc.cc.cc.cc/32 | 0.0.0.0  | imp-null/exp-null  |
| bb.bb.bb.bb/32 | nn.0.0.1 | 20/exp-null        |
| hh.hh.hh.hh/32 | pp.0.0.1 | 26/34              |
| gg.gg.gg.gg/32 | pp.0.0.1 | 23/30              |
| nn.0.0.0       | 0.0.0.0  | imp-null/exp-null  |
| ss.0.0.0       | pp.0.0.1 | 25/33              |
| pp.0.0.0       | 0.0.0.0  | imp-null/exp-null  |
| pp.0.0.1/32    | 0.0.0.0  | 16/exp-null        |

Verify that the prefix of the remote PE router is in the CEF table:

```
Router# show ip cef hh.hh.hh.hh
```

```

hh.hh.hh.hh/32, version 54, cached adjacency pp.0.0.1
0 packets, 0 bytes
tag information set
local tag: 26
fast tag rewrite with Et3/0, pp.0.0.1, tags imposed {34}
via pp.0.0.1, 0 dependencies, recursive
next hop pp.0.0.1, Ethernet3/0 via pp.0.0.1/32
valid cached adjacency
tag rewrite with Et3/0, pp.0.0.1, tags imposed {34}

```

Verify that the prefix of the remote PE router is in the MPLS forwarding table:

```
Router# show mpls forwarding-table hh.hh.hh.hh
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 26        | 34                 | hh.hh.hh.hh/32      | 81786              | Et3/0              | pp.0.0.1 |

```
Router# show mpls forwarding-table hh.hh.hh.hh detail
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
|           |                    |                     |                    |                    |          |

```

26 34 hh.hh.hh.hh/32 81863 Et3/0 pp.0.0.1
 MAC/Encaps=14/18, MTU=1500, Tag Stack{34}
 00B0C26E105500B04A74A0548847 00022000
 No output feature configured
 Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

```

## Configuring the Customer Carrier Network: Examples

Customer carrier configuration and verification examples in this section include:

- [Verifying IP Connectivity in the Customer Carrier: Example, page 45](#)
- [Configuring a Customer Carrier Core Router as a Route Reflector: Example, page 46](#)

### Verifying IP Connectivity in the Customer Carrier: Example

Verify the connectivity from one customer carrier core router to another (from CE1 to CE2) by entering the following command:

```

Router# ping jj.jj.jj.jj

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to jj.jj.jj.jj, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms

```

Verify the path that a packet goes through on its way to its final destination from CE1 to CE2:

```

Router# trace jj.jj.jj.jj

Type escape sequence to abort.
Tracing the route to jj.jj.jj.jj

 1 mm.0.0.2 0 msec 0 msec 4 msec
 2 nn.0.0.2 [MPLS: Labels 20/21 Exp 0] 8 msec 8 msec 12 msec
 3 pp.0.0.2 [MPLS: Labels 28/21 Exp 0] 8 msec 8 msec 12 msec
 4 ss.0.0.1 [MPLS: Labels 17/21 Exp 0] 8 msec 8 msec 12 msec
 5 ss.0.0.2 [MPLS: Labels 16/21 Exp 0] 8 msec 8 msec 12 msec
 6 tt.0.0.1 [AS 200] [MPLS: Label 21 Exp 0] 8 msec 8 msec 8 msec
 7 tt.0.0.2 [AS 200] 8 msec 4 msec *

```

Verify the path that a packet goes through on its way to its final destination from CE2 to CE1:

```

Router# trace aa.aa.aa.aa

Type escape sequence to abort.
Tracing the route to aa.aa.aa.aa

 1 tt.0.0.1 0 msec 0 msec 0 msec
 2 qq.0.0.2 [MPLS: Labels 18/21 Exp 0] 8 msec 12 msec 12 msec
 3 ss.0.0.1 [MPLS: Labels 28/21 Exp 0] 8 msec 8 msec 8 msec
 4 pp.0.0.2 [MPLS: Labels 17/21 Exp 0] 12 msec 8 msec 8 msec
 5 pp.0.0.1 [MPLS: Labels 16/21 Exp 0] 12 msec 12 msec 8 msec
 6 mm.0.0.2 [AS 200] [MPLS: Label 21 Exp 0] 12 msec 8 msec 12 msec
 7 mm.0.0.1 [AS 200] 4 msec 4 msec *

```

## Configuring a Customer Carrier Core Router as a Route Reflector: Example

The following example shows how to use an address family to configure internal BGP peer 10.1.1.1 as a route-reflector client for both unicast and multicast prefixes:

```
router bgp 200
 address-family vpnv4
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 route-reflector-client

router bgp 100
 address-family vpnv4
 neighbor xx.xx.xx.xx activate
 neighbor xx.xx.xx.xx route-reflector-client
 ! xx.xx.xx.xx is a PE router
 neighbor xx.xx.xx.xx send-community extended
 exit address-family
! You need to configure your peer BGP neighbor.
```

## Configuring the Customer Site for Hierarchical VPNs: Examples

This section contains the following configuration and verification examples for the customer site:

- [Configuring PE Routers for Hierarchical VPNs: Examples, page 46](#)
- [Verifying Labels in Each PE Router for Hierarchical VPNs: Examples, page 47](#)
- [Configuring CE Routers for Hierarchical VPNs: Examples, page 48](#)
- [Verifying IP Connectivity in the Customer Site: Examples, page 49](#)

## Configuring PE Routers for Hierarchical VPNs: Examples

This example shows how to configure a PE router:

```
ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Ethernet3/0
 ip address nn.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 mpls ip
!
interface Ethernet3/3
 ip vrf forwarding vpn2
 ip address mm.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
router ospf 200
 log-adjacency-changes
```

```

auto-cost reference-bandwidth 1000
redistribute connected subnets
passive-interface Ethernet3/3
network bb.bb.bb.bb 0.0.0.0 area 200
network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor hh.hh.hh.hh remote-as 200
 neighbor hh.hh.hh.hh update-source Loopback0
!
address-family vpnv4 !VPNv4 session with PE2
 neighbor hh.hh.hh.hh activate
 neighbor hh.hh.hh.hh send-community extended
 bgp dampening 30
 exit-address-family
!
address-family ipv4 vrf vpn2
 neighbor mm.0.0.1 remote-as 300
 neighbor mm.0.0.1 activate
 neighbor mm.0.0.1 as-override
 neighbor mm.0.0.1 advertisement-interval 5
no auto-summary
no synchronization
 bgp dampening 30
 exit-address-family

```

## Verifying Labels in Each PE Router for Hierarchical VPNs: Examples

The following examples show how to verify the configuration of PE router in hierarchical VPNs.

Verify that the loopback address of the local CE router is in the routing table of the PE1 router:

```
Router# show ip route vrf vpn2 aa.aa.aa.aa
```

```

Routing entry for aa.aa.aa.aa/32
 Known via "bgp 200", distance 20, metric 0
 Tag 300, type external
 Last update from mm.0.0.2 20:36:59 ago
 Routing Descriptor Blocks:
 * mm.0.0.2, from mm.0.0.2, 20:36:59 ago
 Route metric is 0, traffic share count is 1
 AS Hops 1, BGP network version 0

```

Verify that the prefix for the local CE router is in the MPLS forwarding table, and that the prefix is untagged:

```
Router# show mpls forwarding-table vrf vpn2 aa.aa.aa.aa
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 23        | Untagged           | aa.aa.aa.aa/32[V]   | 0                  | Et3/3              | mm.0.0.2 |

Verify that the prefix of the remote PE router is in the Cisco Express Forwarding (CEF) table:

```
Router# show ip cef hh.hh.hh.hh
```

```

hh.hh.hh.hh/32, version 31, cached adjacency mn.0.0.2
0 packets, 0 bytes
 tag information set
 local tag: 31

```

```

 fast tag rewrite with Et3/0, nn.0.0.2, tags imposed {26}
 via nn.0.0.2, Ethernet3/0, 2 dependencies
 next hop nn.0.0.2, Ethernet3/0
 unresolved
 valid cached adjacency
 tag rewrite with Et3/0, nn.0.0.2, tags imposed {26}

```

Verify that the loopback address of the remote CE router is in the routing table:

```

Router# show ip route vrf vpn2 jj.jj.jj.jj

Routing entry for jj.jj.jj.jj/32
 Known via "bgp 200", distance 200, metric 0
 Tag 300, type internal
 Last update from hh.hh.hh.hh 20:38:49 ago
 Routing Descriptor Blocks:
 * hh.hh.hh.hh (Default-IP-Routing-Table), from hh.hh.hh.hh, 20:38:49 ago
 Route metric is 0, traffic share count is 1
 AS Hops 1, BGP network version 0

```

Verify that the prefix of the remote CE router is in the MPLS forwarding table, and that an outgoing interface exists:

```

Router# show mpls forwarding-table vrf vpn2 jj.jj.jj.jj

Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
None 26 jj.jj.jj.jj/32 0 Et3/0 nn.0.0.2

```

Verify that the prefix of the remote CE router is in the CEF table:

```

Router# show ip cef vrf vpn2 jj.jj.jj.jj

jj.jj.jj.jj/32, version 12, cached adjacency nn.0.0.2
0 packets, 0 bytes
 tag information set
 local tag: VPN route head
 fast tag rewrite with Et3/0, nn.0.0.2, tags imposed {26 32}
 via hh.hh.hh.hh, 0 dependencies, recursive
 next hop nn.0.0.2, Ethernet3/0 via hh.hh.hh.hh/32
 valid cached adjacency
 tag rewrite with Et3/0, nn.0.0.2, tags imposed {26 32}

```

Verify that the prefix of the local PE router is in the CEF table:

```

Router# show ip cef bb.bb.bb.bb

bb.bb.bb.bb/32, version 9, connected, receive
 tag information set
 local tag: implicit-null

```

## Configuring CE Routers for Hierarchical VPNs: Examples

The following example shows how to configure a CE router:

```

ip cef
interface Loopback0
ip address aa.aa.aa.aa 255.255.255.255
!
interface Ethernet3/3
ip address mm.0.0.1 255.0.0.0
!
router bgp 300
no synchronization

```

```

bgp log-neighbor-changes
timers bgp 10 30
redistribute connected !Redistributing routes into BGP
neighbor mm.0.0.2 remote-as 200 !to send to PE1
neighbor mm.0.0.2 advertisement-interval 5
no auto-summary

```

## Verifying IP Connectivity in the Customer Site: Examples

The following examples show how to verify IP connectivity at the customer site.

Verify that the loopback address of the remote CE router, learned from the PE router, is in the routing table of the local router:

```

Router# show ip route jj.jj.jj.jj

Routing entry for jj.jj.jj.jj/32
 Known via "bgp 300", distance 20, metric 0
 Tag 200, type external
 Redistributing via ospf 300
 Advertised by ospf 300 subnets
 Last update from mm.0.0.1 20:29:35 ago
 Routing Descriptor Blocks:
 * mm.0.0.1, from mm.0.0.1, 20:29:35 ago
 Route metric is 0, traffic share count is 1
 AS Hops 2

```

## Additional References

The following sections provide references related to MPLS VPNs.

### Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                      |
|----------|------------------------------------------------------------|
| RFC 1164 | Application of the Border Gateway Protocol in the Internet |
| RFC 1171 | A Border Gateway Protocol 4                                |
| RFC 1700 | Assigned Numbers                                           |
| RFC 1966 | BGP Route Reflection: An Alternative to Full Mesh IBGP     |
| RFC 2283 | Multiprotocol Extensions for BGP-4                         |
| RFC 2547 | BGP/MPLS VPNs                                              |
| RFC 2842 | Capabilities Advertisement with BGP-4                      |
| RFC 2858 | Multiprotocol Extensions for BGP-4                         |
| RFC 3107 | Carrying Label Information in BGP-4                        |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for MPLS VPN CSC with BGP

Table 2 lists the features in this module and provides links to specific configuration information. Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.


**Note**

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN CSC with BGP

| Feature Name                                                    | Releases                                                                                              | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution | 12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.0(24)S<br>12.2(14)S<br>12.0(27)S<br>12.0(29)S | <p>This feature enables you to create an MPLS VPN CSC network that uses BGP to transport routes and MPLS labels.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About MPLS VPN CSC with BGP, page 2</a></li> <li>• <a href="#">How to Configure MPLS VPN CSC with BGP, page 5</a></li> </ul> |

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN

---

Route maps enable you to specify which routes are distributed with Multiprotocol Label Switching (MPLS) labels. Route maps also enable you to specify which routes with MPLS labels a router receives and adds to its Border Gateway Protocol (BGP) table.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for Route Maps in MPLS VPNs”](#) section on page 13.

## Contents

- [Restrictions for Using Route Maps with MPLS VPNs, page 2](#)
- [Prerequisites for Using Route Maps with MPLS VPNs, page 2](#)
- [Information About Route Maps in MPLS VPNs, page 2](#)
- [How to Configure Route Maps in an MPLS VPN, page 2](#)
- [Configuration Examples for Route Maps in MPLS VPNs, page 8](#)
- [Additional References, page 11](#)
- [Feature Information for Route Maps in MPLS VPNs, page 13](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Restrictions for Using Route Maps with MPLS VPNs

You can use route maps with MPLS VPN Inter-AS with Autonomous System Boundary Routers (ASBRs) exchanging IPv4 routes with MPLS labels. You cannot use route maps with MPLS VPN Inter-AS with ASBRs exchanging VPN-IPv4 addresses.

## Prerequisites for Using Route Maps with MPLS VPNs

Before you configure and apply route maps, you need to create an access control list (ACL) and specify the routes that the router should distribute with MPLS labels.

## Information About Route Maps in MPLS VPNs

When routers are configured to distribute routes with MPLS labels, all the routes are encoded with the multiprotocol extensions and contain MPLS labels. You can use a route map to control the distribution of MPLS labels between routers.

Route maps enable you to specify which routes are distributed with MPLS labels. Route maps also enable you to specify which routes with MPLS labels a router receives and adds to its BGP table. Route maps enable you to specify the following:

- For a router distributing MPLS labels, you can specify which routes are distributed with an MPLS label.
- For a router receiving MPLS labels, you can specify which routes are accepted and installed in the BGP table.

Route maps work with ACLs. You enter the routes into an ACL and then specify the ACL when you configure the route map. You can configure a router to accept only routes that are specified in the route map. The router checks the routes listed in the BGP update message against the list of routes in the specified ACL. If a route in the BGP update message matches a route in the ACL, the route is accepted and added to the BGP table.

## How to Configure Route Maps in an MPLS VPN

Perform the following tasks to enable routers to send MPLS labels with the routes specified in the route maps:

- [Configuring a Route Map for Incoming Routes, page 2](#) (optional)
- [Configuring a Route Map for Outgoing Routes, page 4](#) (optional)
- [Applying the Route Maps to the MPLS VPN Edge Routers, page 6](#) (optional)

## Configuring a Route Map for Incoming Routes

Perform this task to create a route map to filter arriving routes. You create an ACL and specify the routes that the router should accept and add to the BGP table.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **route-map** *map-name* [**permit** | **deny**] *sequence-number*
5. **match ip address** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
6. **match mpls-label**
7. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                               | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                  | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                                                                                                                                                                                           |
| Step 4 | <b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] <i>sequence-number</i><br><br><b>Example:</b><br>Router(config-router)# route-map csc-mpls-routes-in permit | Enters route map configuration mode and creates a route map with the name you specify. <ul style="list-style-type: none"> <li>• The <i>map-name</i> argument identifies the name of the route map.</li> <li>• The <b>permit</b> keyword allows the actions to happen if all conditions are met.</li> <li>• A <b>deny</b> keyword prevents any actions from happening if all conditions are met.</li> <li>• The <i>sequence-number</i> argument allows you to prioritize route maps. If you have multiple route maps and want to prioritize them, assign each one a number. The route map with the lowest number is implemented first, followed by the route map with the second lowest number, and so on.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>match ip address {access-list-number [access-list-number...   access-list-name...]   access-list-name [access-list-number...   access-list-name]   prefix-list prefix-list-name [prefix-list-name...]}</pre> <p><b>Example:</b><br/>Router(config-route-map)# match ip address<br/>acl-in</p> | <p>Distributes any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or performs policy routing on packets.</p> <ul style="list-style-type: none"> <li>The <i>access-list-number...</i> argument is a number of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.</li> <li>The <i>access-list-name...</i> argument is a name of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.</li> <li>The <b>prefix-list</b> keyword distributes routes based on a prefix list.</li> <li>The <i>prefix-list-name...</i> argument is a name of a specific prefix list. The ellipsis indicates that multiple values can be entered.</li> </ul> |
| Step 6 | <pre>match mpls-label</pre> <p><b>Example:</b><br/>Router(config-route-map)# match mpls-label</p>                                                                                                                                                                                                  | <p>Redistributes routes that include MPLS labels if the routes meet the conditions specified in the route map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 7 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-route-map)# exit</p>                                                                                                                                                                                                                          | <p>Exits route map configuration mode and returns to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Configuring a Route Map for Outgoing Routes

This configuration is optional.

Perform this task to create a route map to filter departing routes. You create an access list and specify the routes that the router should distribute with MPLS labels.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **route-map** *map-name* [**permit** | **deny**] *sequence-number*
5. **match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }
6. **set mpls-label**
7. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                   | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                              | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <p><b>router bgp</b> <i>as-number</i></p> <p><b>Example:</b><br/>Router(config)# router bgp 100</p>                                                                                 | <p>Configures a BGP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul> <p>Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</p>                                                                                                                                                                                                                                                              |
| Step 4 | <p><b>route-map</b> <i>map-name</i> [<b>permit</b>   <b>deny</b>] <i>sequence-number</i></p> <p><b>Example:</b><br/>Router(config-router)# route-map csc-mpls-routes-out permit</p> | <p>Enters route map configuration mode and creates a route map with the name you specify.</p> <ul style="list-style-type: none"> <li>The <i>map-name</i> argument identifies the name of the route map.</li> <li>The <b>permit</b> keyword allows the actions to happen if all conditions are met.</li> <li>A <b>deny</b> keyword prevents any actions from happening if all conditions are met.</li> <li>The <i>sequence-number</i> argument allows you to prioritize route maps. If you have multiple route maps and want to prioritize them, assign each one a number. The route map with the lowest number is implemented first, followed by the route map with the second lowest number, and so on.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>match ip address {access-list-number [access-list-number...   access-list-name...]   access-list-name [access-list-number...  access-list-name]   prefix-list prefix-list-name [prefix-list-name...]}</pre> <p><b>Example:</b><br/>Router(config-route-map)# match ip address<br/>acl-out</p> | <p>Distributes any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or performs policy routing on packets.</p> <ul style="list-style-type: none"> <li>The <i>access-list-number...</i> argument is a number of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.</li> <li>The <i>access-list-name...</i> argument is a name of a standard or extended access list. It can be an integer from 1 to 199. The ellipsis indicates that multiple values can be entered.</li> <li>The <b>prefix-list</b> keyword distributes routes based on a prefix list.</li> <li>The <i>prefix-list-name...</i> argument is a name of a specific prefix list. The ellipsis indicates that multiple values can be entered.</li> </ul> |
| Step 6 | <pre>set mpls-label</pre> <p><b>Example:</b><br/>Router(config-route-map)# set mpls-label</p>                                                                                                                                                                                                      | <p>Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7 | <pre>exit</pre> <p>Router(config-route-map)# exit</p>                                                                                                                                                                                                                                              | <p>Exits route map configuration mode and returns to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Applying the Route Maps to the MPLS VPN Edge Routers

This configuration is optional.

Perform this task to enable the edge routers to use the route maps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** *ip-address* **route-map** *route-map-name* **in**
6. **neighbor** *ip-address* **route-map** *route-map-name* **out**
7. **neighbor** *ip-address* **send-label**
8. **exit-address-family**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                           | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <p><b>router bgp as-number</b></p> <p><b>Example:</b><br/>Router(config)# router bgp 100</p>                                                                     | <p>Configures a BGP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                    |
| Step 4 | <p><b>address-family ipv4 [multicast   unicast   vrf vrf-name]</b></p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf vpn1</p>            | <p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <p><b>neighbor ip-address route-map map-name in</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1 route-map csc-mpls-routes-in in</p>   | <p>Applies a route map to incoming routes.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the router to which the route map is to be applied.</li> <li>The <i>map-name</i> argument specifies the name of the route map.</li> <li>The <b>in</b> keyword applies the route map to incoming routes.</li> </ul>                                                                                                                  |
| Step 6 | <p><b>neighbor ip-address route-map map-name out</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1 route-map csc-mpls-route-out out</p> | <p>Applies a route map to outgoing routes.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the router to which the route map is to be applied.</li> <li>The <i>map-name</i> argument specifies the name of the route map.</li> <li>The <b>out</b> keyword applies the route map to outgoing routes.</li> </ul>                                                                                                                 |

|        | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <code>neighbor ip-address send-label</code><br><br><b>Example:</b><br>Router(config-router-af)# neighbor pp.0.0.1<br>send-label | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul> |
| Step 8 | <code>exit-address-family</code><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                        | Exits from address family configuration mode.                                                                                                                                                                              |
| Step 9 | <code>end</code><br><br><b>Example:</b><br>Router(config-router)# end                                                           | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                  |

### Troubleshooting Tips

You can enter a **show route-map** *map-name* command to verify that the route map is applied to the PE routers.



#### Note

After you make any changes to a route map, you need to reset the BGP connection for the changes to take effect.

## Configuration Examples for Route Maps in MPLS VPNs

This section includes the following MPLS VPN route map examples:

- [Using a Route Map in an MPLS VPN Inter-AS Network: Example, page 8](#)
- [Using a Route Map in an MPLS VPN CSC Network: Example, page 10](#)

### Using a Route Map in an MPLS VPN Inter-AS Network: Example

In this example, a route map is applied to an autonomous system border router (ASBR) that exchanges IPv4 routes and MPLS labels with another ASBR.

- A route map called OUT specifies that the ASBR should distribute the PE1 route (ee.ee) with labels and the RR1 route (aa.aa) without labels.
- A route map called IN specifies that the ASBR should accept the PE2 route (ff.ff) with labels and the RR2 route (bb.bb) without labels.

```
ip subnet-zero
mpls label protocol tdp
!
interface Loopback0
 ip address ww.ww.ww.ww 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
```

```

!
interface Ethernet0/2
 ip address hh.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet0/3
 ip address dd.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 tag-switching ip
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network ww.ww.ww.ww 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100

router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor hh.0.0.1 remote-as 200
 no auto-summary
!
!
address-family ipv4
 redistribute ospf 10
 neighbor aa.aa.aa.aa activate
 neighbor aa.aa.aa.aa send-label
 neighbor hh.0.0.1 activate
 neighbor hh.0.0.1 advertisement-interval 5
 neighbor hh.0.0.1 send-label
 neighbor hh.0.0.1 route-map IN in
 neighbor hh.0.0.1 route-map OUT out
 neighbor kk.0.0.1 activate
 neighbor kk.0.0.1 advertisement-interval 5
 neighbor kk.0.0.1 send-label
 neighbor kk.0.0.1 route-map IN in
 neighbor kk.0.0.1 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ee.ee.ee.ee log
access-list 2 permit ff.ff.ff.ff log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log

route-map IN permit 10
 match ip address 2
 match mpls-label
!
route-map IN permit 11
 match ip address 4
!
route-map OUT permit 12

```

```

 match ip address 3
 !
route-map OUT permit 13
 match ip address 1
 set mpls-label
 !
end

```

## Using a Route Map in an MPLS VPN CSC Network: Example

The following example creates two route maps, which are named:

- IN for incoming routes
- OUT for outgoing routes

The route maps specify the following:

- If an IP address in an incoming BGP update message matches an IP address in access list 99, the route is added to the BGP table.
- If an IP address in an outbound BGP update message matches an IP address in access list 88, the router distributes that route.

The route maps are applied to the CSC-PE router with the address qq.0.0.1.

```

address-family ipv4 vrf vpn2
 neighbor qq.0.0.1 remote-as 200
 neighbor qq.0.0.1 activate
 neighbor qq.0.0.1 as-override
 neighbor qq.0.0.1 advertisement-interval 5
 neighbor qq.0.0.1 route-map IN in
 neighbor qq.0.0.1 route-map OUT out
 neighbor qq.0.0.1 send-label
 !
access-list 88 permit rr.rr.rr.rr
access-list 88 permit ss.ss.ss.ss
access-list 88 permit tt.tt.tt.tt
access-list 99 permit uu.uu.uu.uu
access-list 99 permit vv.vv.vv.vv
access-list 99 permit ww.ww.ww.ww
 !
route-map IN permit 1
 match ip address 99
 !
route-map OUT permit 1
 match ip address 88
 set mpls-label
 !

```

## Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic MPLS VPNs                     | <a href="#">Configuring MPLS Layer 3 VPNs</a><br><a href="#">Configuring Scalable Hub-and-Spoke MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a></li> <li>• <a href="#">Preserving QoS Settings in an MPLS VPN Carrier Supporting Carrier Network</a></li> <li>• <a href="#">Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</a></li> </ul> |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> </ul>                                                                                                                                                                                                          |
| MPLS VPN load sharing               | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN MIBs                       | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Directing MPLS VPN traffic          | <ul style="list-style-type: none"> <li>• <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a></li> <li>• <a href="#">Directing MPLS VPN Traffic Using a Source IP Address</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| VPN ID                              | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Dialer applications with MPLS VPNs  | <a href="#">Dialing to Destinations with the Same IP Address for MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MPLS VPNs and OSPF                  | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for Route Maps in MPLS VPNs

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Route Maps in MPLS VPNs

| Feature Name                                                                                                                                                                                                                                                 | Releases                                                                                              | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| This feature was included as part of the following features: <ul style="list-style-type: none"> <li>MPLS VPN Inter-Autonomous Systems - IPv4 BGP Label Distribution</li> <li>MPLS VPN Carrier Supporting Carrier with IPv4 BGP Label Distribution</li> </ul> | 12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.0(24)S<br>12.2(14)S<br>12.0(27)S<br>12.0(29)S | Route maps enable you to specify which routes are distributed with MPLS labels. Route maps also enable you to specify which routes with MPLS labels a router receives and adds to its BGP table.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">Information About Route Maps in MPLS VPNs, page 2</a></li> <li><a href="#">How to Configure Route Maps in an MPLS VPN, page 2</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# Load Sharing MPLS VPN Traffic

---

**First Published: May 02, 2005**

**Last Updated: July 11, 2008**

Load sharing distributes traffic so that no individual router is overburdened. In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) network, you can achieve load sharing through the following methods:

- BGP Multipath options
- Directly Connected Loopback Peering

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Load Sharing MPLS VPN Traffic](#)” section on page 48.

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Load Sharing MPLS VPN Traffic, page 2](#)
- [Restrictions for Load Sharing MPLS VPN Traffic, page 2](#)
- [Information About Load Sharing MPLS VPN Traffic, page 4](#)
- [How to Configure Load Sharing, page 7](#)
- [Additional References, page 47](#)
- [Feature Information for Load Sharing MPLS VPN Traffic](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

## Prerequisites for Load Sharing MPLS VPN Traffic

Before configuring load sharing, ensure that your MPLS VPN network (including MPLS VPN Carrier Supporting Carrier or interautonomous System) is configured and working properly. See the “[Related Documents](#)” section on page 47 for references related to MPLS VPNs.

## Restrictions for Load Sharing MPLS VPN Traffic

When static routes are configured in an MPLS or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.nT, 12.nM, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later releases. Use the following guidelines when configuring static routes.

### Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in an MPLS environment:

```
ip route destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

### Unsupported Static Routes in an MPLS Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

```
ip route destination-prefix mask next-hop1
ip route destination-prefix mask next-hop2
```

Use the *interface* and *next-hop* arguments when specifying static routes.

### Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are associated with the same Virtual Routing and Forwarding (VRF) instance:

- **ip route vrf** vrf-name destination-prefix mask next-hop-address
- **ip route vrf** vrf-name destination-prefix mask interface next-hop-address

- **ip route vrf** *vrf-name destination-prefix mask interface1 next-hop1*  
**ip route vrf** *vrf-name destination-prefix mask interface2 next-hop2*

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the internet gateway.

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address global*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*  
(This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

#### Unsupported Static Routes in an MPLS VPN Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

```
ip route vrf destination-prefix mask next-hop-address global
```

The following **ip route** commands are not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

```
ip route vrf destination-prefix mask next-hop1 global
ip route vrf destination-prefix mask next-hop2 global
```

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

```
ip route vrf vrf-name destination-prefix mask next-hop1
ip route vrf vrf-name destination-prefix mask next-hop2
```

#### Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table on the Customer Edge (CE) side. For example, the following command is supported when the destination-prefix is the CE router's loopback address, as in EBGp multihop cases.

```
ip route vrf vrf-name destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 nexthop1
ip route destination-prefix mask interface2 nexthop2
```

# Information About Load Sharing MPLS VPN Traffic

Before configuring load sharing features, you should understand the following concepts:

- [Load Sharing Using BGP Multipath Options, page 4](#)
- [Load Sharing Using Directly Connected Loopback Peering, page 6](#)

## Load Sharing Using BGP Multipath Options

A variety of Border Gateway Protocol (BGP) Multipath options exist that enable you to configure load sharing on your MPLS VPN that uses BGP. The following sections describe some BGP Multipath options:

- [Internal BGP Multipath Load Sharing, page 4](#)
- [BGP Multipath for eBGP and iBGP, page 4](#)
- [eBGP Multipath Load Sharing, page 6](#)

### Internal BGP Multipath Load Sharing

When a BGP-speaking router with no local policy configured receives multiple Network Layer Reachability Information (NLRI) from the internal BGP (iBGP) for the same destination, the router chooses one iBGP path as the best path. The best path is then installed in the IP routing table of the router. The iBGP Multipath feature enables the BGP-speaking router to select multiple iBGP paths as the best paths to a destination. The best paths are then installed in the IP routing table of the router. To enable iBGP Multipath load sharing, you issue the **maximum-paths ibgp** command in router configuration mode. For more information about iBGP Multipath load sharing, see [Configuring BGP](#).

### BGP Multipath for eBGP and iBGP

The BGP Multipath load sharing for both eBGP and iBGP in an MPLS VPN feature allows multihomed autonomous systems and provider edge (PE) routers to be configured to distribute traffic across both external BGP (eBGP) and iBGP paths.

BGP installs up to the maximum number of paths allowed (configured using the **maximum-paths** command). BGP uses the best path algorithm to select one multipath as the best path, inserts the best path into the Routing Information Base (RIB), and advertises the best path to BGP peers. Other multipaths may be inserted into the RIB, but only one path is selected as the best path.

The multipaths are used by Cisco Express Forwarding to perform load balancing, which can be performed on a per-packet or per-source or destination pair basis. To enable the load sharing feature, configure the router with MPLS VPNs that contain VPN routing and forwarding instances (VRFs) that import both eBGP and iBGP paths. The number of multipaths can be configured separately for each VRF.

**Note**

---

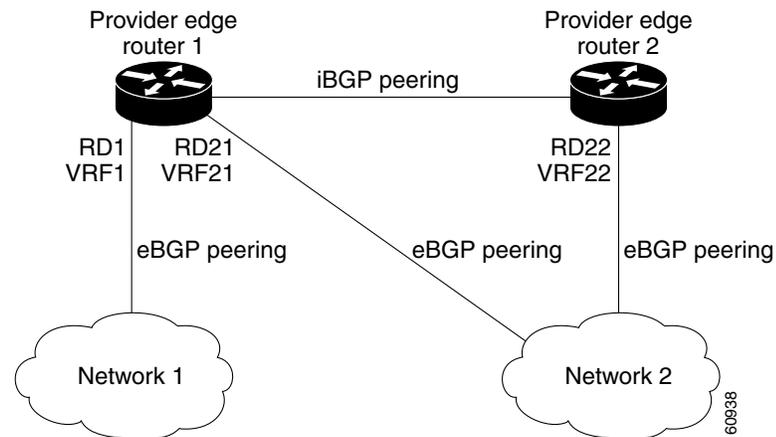
This feature operates within the configuration parameters of the existing outbound routing policy.

---

## eBGP and iBGP Multipath Load Sharing in an MPLS Network using BGP

Figure 1 shows an MPLS service provider network using BGP that connects two remote networks to PE1 and PE2, which are both configured for VPNv4 unicast iBGP peering. Network 2 is a multihomed network that is connected to PE1 and PE2. Network 2 also has extranet VPN services configured with Network 1. Both Network 1 and Network 2 are configured for eBGP peering with the PE routers.

**Figure 1** A Service Provider MPLS Network Using BGP



PE1 can be configured so that both iBGP and eBGP paths can be selected as multipaths and imported into the VRF of Network 1. The multipaths will be used by Cisco Express Forwarding to perform load balancing. Traffic is distributed as follows:

- IP traffic that is sent from Network 2 to PE1 and PE2 is sent across the eBGP paths as IP traffic.
- IP traffic that is sent from PE1 to PE2 is sent across the iBGP path as MPLS traffic.
- MPLS traffic that is sent across an eBGP path is sent as IP traffic.

Any prefix that is advertised from Network 2 will be received by PE1 through route distinguisher (RD) 21 and RD22.

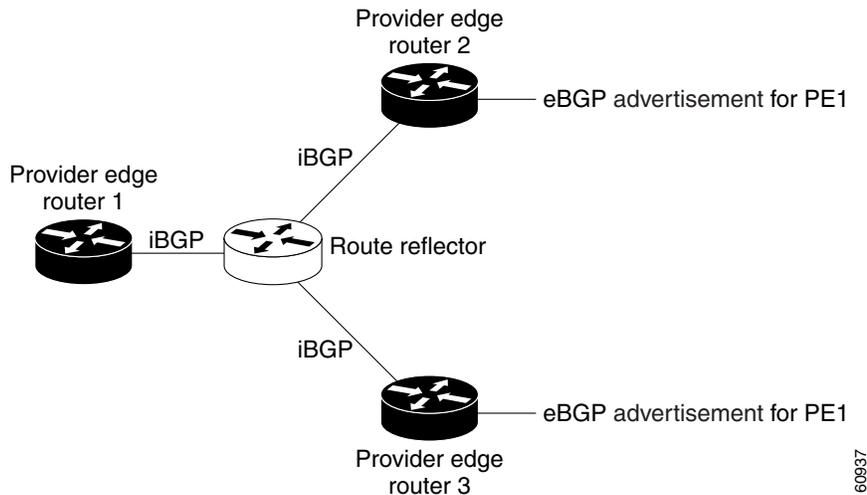
- The advertisement through RD21 is carried in IP packets.
- The advertisement through RD22 is carried in MPLS packets.

Both paths can be selected as multipaths for VRF1 and inserted into the VRF1 RIB.

## eBGP and iBGP Multipath Load Sharing with Route Reflectors

Figure 2 shows a topology that contains three PE routers and a route reflector, all configured for iBGP peering. PE2 and PE3 each advertise an equal preference eBGP path to PE1. By default, the route reflector chooses only one path and advertises PE1.

**Figure 2** *Topology with a Route Reflector*



For all equal preference paths to PE1 to be advertised through the route reflector, you must configure each VRF with a different RD. The prefixes received by the route reflector are recognized differently and advertised to PE1.

## eBGP Multipath Load Sharing

When a router learns two identical eBGP paths for a prefix from a neighboring autonomous system (AS), it will choose the path with the lowest route ID as the best path. This best path is installed in the IP routing table. You can enable eBGP Multipath, which installs multiple paths in the IP routing table when the eBGP paths are learned from a neighboring Autonomous System (AS), instead of picking one best path.

During packet switching, depending on the switching mode, either per-packet or per-destination load sharing is performed among the multiple paths. The **maximum-paths** router configuration command controls the number of paths allowed. By default, BGP will install only one path to the IP routing table.

## Load Sharing Using Directly Connected Loopback Peering

You use this feature with MPLS VPN Inter-AS and MPLS VPN Content Security and Control (CSC) networks to load share traffic between adjacent label switched routers (LSRs) that are connected by multiple links. The LSRs could be a pair of Autonomous System Boundary Routers (ASBRs) or a CSC-PE and a CSC-CE.

Using directly connected loopback peering allows load sharing at the IGP level, so more than one BGP session is not needed between the LSRs. No other label distribution mechanism is needed between the adjacent LSRs than BGP.

Directly connected loopback peering enables load sharing of traffic as follows:

- A BGP session is established, using the loopback addresses of the LSRs.
- MPLS is enabled on the connecting links.
- Multiple static routes to the loopback address of the adjacent LSR allow IGP load sharing.
- The outgoing label to the loopback address of the adjacent LSR is an implicit null label and is inferred by the LSR.

- Because IGP load sharing is enabled on the loopback address of the adjacent LSR, any traffic destined to a prefix that is learned over the BGP session (and recurses over the loopback) is load shared.

## How to Configure Load Sharing

This section contains the following procedures:

- [Configuring BGP Multipath Load Sharing for eBGP and iBGP, page 7](#)
- [Verifying BGP Multipath Load Sharing for eBGP and iBGP, page 8](#)
- [Configuring eBGP Multipath Load Sharing with MPLS VPN Inter-AS, page 9](#)
- [Configuring eBGP Multipath Load Sharing with MPLS VPN Carrier Supporting Carrier, page 11](#)
- [Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS using ASBRs to Exchange VPN-IPv4 Addresses, page 16](#)
- [Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS Using ASBRs to Exchange IPv4 Routes and Labels, page 24](#)
- [Configuring Directly Connected Loopback Peering on MPLS VPN Carrier Supporting Carrier, page 32](#)

## Configuring BGP Multipath Load Sharing for eBGP and iBGP

### Restrictions

- Configuring BGP Multipath for eBGP and iBGP is only for basic MPLS Layer 3 VPNs. MPLS VPN Inter-AS and MPLS VPN Carrier Supporting Carrier do not support this multipath configuration.
- With multiple iBGP paths installed in a routing table, a route reflector will advertise only one of the paths (one next hop). If a router is behind a route reflector, all routers that are connected to multihomed sites will not be advertised unless separate VRFs with different RDs are configured for each VRF.
- Each IP routing table entry for a BGP prefix that has multiple iBGP paths uses additional memory. We recommend not using this feature on a router with a low amount of available memory and especially when the router is carrying a full Internet routing table.

To configure iBGP and eBGP routes for multipath load sharing, perform the following task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **maximum-paths eibgp** *number-of-paths*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 1                                                                                   | Enters router configuration mode and configures the router to run a BGP routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vrf1 | Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv4 address prefixes.<br><br><b>Note</b> For this task you must create the vrf and specify the <b>vrf</b> keyword. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>maximum-paths eibgp</b> <i>number-of-paths</i><br><br><b>Example:</b><br>Router(config-router-af)# maximum-paths eibgp 6                                                 | Configures the number of parallel iBGP and eBGP routes that can be installed into a routing table.<br><br><b>Note</b> Configure the <b>maximum-paths eibgp</b> command in address family ipv4 vrf configuration mode.                                                                                                                                                                                                                                                                                                                                                                                     |

## Verifying BGP Multipath Load Sharing for eBGP and iBGP

To verify the configuration of iBGP and eBGP routes for multipath load sharing, perform this task.

## SUMMARY STEPS

- enable**
- show ip bgp vpnv4 ip-address**

## DETAILED STEPS

|        | Command or Action                                                                                 | Purpose                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show ip bgp vpnv4 ip-prefix</b><br><br><b>Example:</b><br>Router# show ip bgp vpnv4 10.0.0.0/8 | Displays attributes and multipaths for a specific network in an MPLS VPN.                                          |

## Example

If you enter the **all** keyword with the **show ip bgp vpnv4** command, the output displays information about all VPN network layer reachability information (NLRI)s for a specified network:

```
Router# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 10:1:22.22.22.0/24, version 19
Paths:(5 available, best #5)
Multipath: eiBGP
 Advertised to non peer-group peers:
 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5
 22
 10.0.0.2 (metric 20) from 10.0.0.4 (10.0.0.4)
 Origin IGP, metric 0, localpref 100, valid, internal, multipath
 Extended Community:0x0:0:0 RT:100:1 0x0:0:0
 Originator:10.0.0.2, Cluster list:10.0.0.4
 22
 10.0.0.2 (metric 20) from 10.0.0.5 (10.0.0.5)
 Origin IGP, metric 0, localpref 100, valid, internal, multipath
 Extended Community:0x0:0:0 RT:100:1 0x0:0:0
 Originator:10.0.0.2, Cluster list:10.0.0.5
 22
 10.0.0.2 (metric 20) from 10.0.0.2 (10.0.0.2)
 Origin IGP, metric 0, localpref 100, valid, internal, multipath
 Extended Community:RT:100:1 0x0:0:0
 22
 10.0.0.2 (metric 20) from 10.0.0.3 (10.0.0.3)
 Origin IGP, metric 0, localpref 100, valid, internal, multipath
 Extended Community:0x0:0:0 RT:100:1 0x0:0:0
 Originator:10.0.0.2, Cluster list:10.0.0.3
 22
 10.1.1.12 from 10.1.1.12 (10.22.22.12)
 Origin IGP, metric 0, localpref 100, valid, external, multipath, best
 Extended Community:RT:100:1
```

## Configuring eBGP Multipath Load Sharing with MPLS VPN Inter-AS

Perform this task on the ASBRs to configure eBGP Multipath for MPLS VPN interautonomous systems with ASBRs exchanging IPv4 routes and MPLS labels.

## Restrictions

eBGP Multipath is not supported on MPLS VPN Inter-AS with ASBRs that exchange VPNv4 routes.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **maximum paths** *number-paths*
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** *ip-address* **send-label**
9. **exit-address-family**
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                             | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                    |

|         | Command or Action                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <p><b>address-family ipv4</b> [<b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4</p> | <p>Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv4 address prefixes.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 6  | <p><b>maximum-paths</b> <i>number-paths</i></p> <p><b>Example:</b><br/>Router(config-router-af)# maximum-paths 2</p>                                                     | <p>(Optional) Controls the maximum number of parallel routes an IP routing protocol can support.</p> <ul style="list-style-type: none"> <li>The <i>number-paths</i> argument specifies the maximum number of parallel routes an IP routing protocol installs in a routing table.</li> </ul>                                                                                                                                                                                                                         |
| Step 7  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.1 activate</p>  | <p>Enables the exchange of information with a neighboring router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                               |
| Step 8  | <p><b>neighbor</b> <i>ip-address</i> <b>send-label</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.1 send-label</p>                             | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                                                                                                                                                   |
| Step 9  | <p><b>exit-address-family</b></p> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                               | <p>Exits from address family configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 10 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                               | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Configuring eBGP Multipath Load Sharing with MPLS VPN Carrier Supporting Carrier

This section contains the following procedures:

- [Configuring eBGP Multipath Load Sharing on the CSC-PE Routers, page 12](#)
- [Configuring eBGP Multipath Load Sharing on the CSC-CE Routers, page 14](#)

## Configuring eBGP Multipath Load Sharing on the CSC-PE Routers

Perform this task to configure eBGP Multipath load sharing on the CSC-PE routers that distribute BGP routes with MPLS labels.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **maximum paths** *number-paths*
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** *ip-address* **as-override**
9. **neighbor** *ip-address* **send-label**
10. **exit-address-family**
11. **end**

### DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100 | Configures a BGP routing process and enters router configuration mode.<br><ul style="list-style-type: none"><li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li></ul> |

|        | Command or Action                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <p><b>address-family ipv4</b> [<b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf vpn1</p>              | <p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <p><b>maximum-paths</b> <i>number-paths</i></p> <p><b>Example:</b><br/>Router(config-router-af)# maximum-paths 2</p>                                                                           | <p>(Optional) Controls the maximum number of parallel routes an IP routing protocol can support.</p> <ul style="list-style-type: none"> <li>On the CSC-PE router, this command is enabled in address family configuration mode.</li> <li>The <i>number-paths</i> argument specifies the maximum number of parallel routes an IP routing protocol installs in a routing table.</li> </ul>                                                                                  |
| Step 6 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>remote-as</b> <i>as-number</i></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.1 remote-as 200</p> | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                |
| Step 7 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.1 activate</p>                        | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                                 |
| Step 8 | <p><b>neighbor</b> <i>ip-address</i> <b>as-override</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.1 as-override</p>                                                 | <p>Configures a PE router to override the autonomous system number (ASN) of a site with the ASN of a provider.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the router that is to be overridden with the ASN provided.</li> </ul>                                                                                                                                                                                |
| Step 9 | <p><b>neighbor</b> <i>ip-address</i> <b>send-label</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.1 send-label</p>                                                   | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                                                                                                         |

|         | Command or Action                                                                                  | Purpose                                   |
|---------|----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 10 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family | Exits address family configuration mode.  |
| Step 11 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                    | (Optional) Exits to privileged EXEC mode. |

## Configuring eBGP Multipath Load Sharing on the CSC-CE Routers

Perform this task to configure eBGP Multipath load sharing on the CSC-CE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **maximum paths** *number-paths*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **redistribute** *protocol*
7. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
8. **neighbor** {*ip-address* | *peer-group-name*} **activate**
9. **neighbor** *ip-address* **send-label**
10. **exit-address-family**
11. **end**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|        | Command or Action                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>router bgp as-number</pre> <p><b>Example:</b><br/>Router(config)# router bgp 200</p>                                                 | <p>Configures a BGP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 4 | <pre>maximum-paths number-paths</pre> <p><b>Example:</b><br/>Router(config-router)# maximum-paths 2</p>                                   | <p>(Optional) Controls the maximum number of parallel routes an IP routing protocol can support.</p> <ul style="list-style-type: none"> <li>On the CSC-CE routers, this command is issued in router configuration mode.</li> <li>The <i>number-paths</i> argument specifies the maximum number of parallel routes an IP routing protocol installs in a routing table.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 5 | <pre>address-family ipv4 [multicast   unicast   vrf vrf-name]</pre> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4</p> | <p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 6 | <pre>redistribute protocol</pre> <p><b>Example:</b><br/>Router(config-router-af)# redistribute static</p>                                 | <p>Redistributes routes from one routing domain into another routing domain.</p> <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b>, <b>connected</b>, <b>egp</b>, <b>igrp</b>, <b>isis</b>, <b>mobile</b>, <b>ospf</b>, <b>rip</b>, and <b>static [ip]</b>. <ul style="list-style-type: none"> <li>The <b>static [ip]</b> keyword redistributes IP static routes.</li> </ul> </li> </ul> <p><b>Note</b> The optional <b>ip</b> keyword is used when you redistribute static routes into Intermediate System-to-Intermediate System (IS-IS).</p> <ul style="list-style-type: none"> <li>The <b>connected</b> keyword refers to routes that are established automatically when IP is enabled on an interface.</li> <li>For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes are redistributed as external to the autonomous system.</li> </ul> |

|         | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <pre>neighbor {ip-address   peer-group-name} remote-as as-number</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.2<br/>remote-as 100</p> | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 8  | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.2<br/>activate</p>                 | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 9  | <pre>neighbor ip-address send-label</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.2<br/>send-label</p>                                 | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                          |
| Step 10 | <pre>exit-address-family</pre> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                         | <p>Exits from the address family configuration mode.</p>                                                                                                                                                                                                                                                                                                                                   |
| Step 11 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-router)# end</p>                                                                                            | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                           |

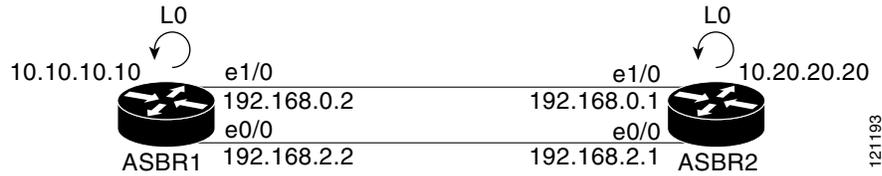
## Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS using ASBRs to Exchange VPN-IPv4 Addresses

This section describes the following tasks you need to do to configure peering of loopback interfaces of directly connected ASBRs:

- [Configuring Loopback Interface Addresses for Directly Connected ASBRs, page 17](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback, page 18](#) (required)
- [Configuring Forwarding on Connecting Loopback Interfaces, page 19](#) (required)
- [Configuring an eBGP Session Between the Loopbacks, page 20](#) (required)
- [Verifying That Load Sharing Occurs Between Loopbacks, page 23](#) (optional)

Figure 3 shows the loopback configuration for directly connected ASBR1 and ASBR2 routers. This configuration is used as the example in the tasks that follow.

**Figure 3** Loopback Interface Configuration for Directly Connected ASBR1 and ASBR2 Routers



121193

## Configuring Loopback Interface Addresses for Directly Connected ASBRs

Perform this task to configure loopback interface addresses for directly connected ASBRs.



**Note**

Loopback addresses need to be configured for each directly connected ASBR. That is, configure a loopback address for ASBR1 and for ASBR2 in the example (see [Figure 3](#)).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address mask* [**secondary**]
5. **end**

### DETAILED STEPS

|        | Command or Action                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                  | Enters global configuration mode.                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>interface loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface loopback0 | Configures a software-only virtual interface that emulates an interface that is always up.<br><ul style="list-style-type: none"><li>The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li></ul> |

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <p><b>ip address</b> <i>ip-address mask [secondary]</i></p> <p><b>Example:</b><br/> Router(config-if)# ip address 10.10.10.10<br/> 255.255.255.255</p> | <p>Sets a primary or secondary IP address for an interface.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 5 | <p><b>end</b></p> <p><b>Example:</b><br/> Router(config-if)# end</p>                                                                                   | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback

Perform the following task to configure /32 static routes on each of the directly connected ASBRs.

### SUMMARY STEPS

- enable**
- configure terminal**
- ip route** *prefix mask {ip-address | interface-type interface-number [ip-address]}*  
[*distance*] [*name*] [**permanent**] [**tag tag**]
- end**

### DETAILED STEPS

|        | Command or Action                                                                       | Purpose                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/> Router&gt; enable</p>                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/> Router# configure terminal</p> | <p>Enters global configuration mode.</p>                                                                                |

|        | Command or Action                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>ip route prefix mask {ip-address   interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]</pre> <p><b>Example:</b><br/> Router(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1</p> | <p>Establishes static routes.</p> <ul style="list-style-type: none"> <li>• The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>• The <i>mask</i> argument is the prefix mask for the destination.</li> <li>• The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the specified network.</li> <li>• The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>• The <i>distance</i> argument is an administrative distance.</li> <li>• The <i>name</i> argument applies a name to the specified route.</li> <li>• The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>• The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution through the use of route maps.</li> </ul> |
| Step 4 | <pre>end</pre> <p><b>Example:</b><br/> Router(config)# end</p>                                                                                                                                                                               | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuring Forwarding on Connecting Loopback Interfaces

Perform this task to configure forwarding on the connecting loopback interfaces.

This task is required for sessions between loopbacks. In the “[Configuring /32 Static Routes to the eBGP Neighbor Loopback](#)” task, Ethernet 1/0 and Ethernet 0/0 are the connecting interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mpls bgp forwarding**
5. **exit**
6. Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code>                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <code>interface type slot/port</code><br><br><b>Example:</b><br><code>Router(config)# interface ethernet 1/0</code> | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |
| Step 4 | <code>mpls bgp forwarding</code><br><br><b>Example:</b><br><code>Router(config-if)# mpls bgp forwarding</code>      | Configures BGP to enable MPLS forwarding on connecting interfaces.                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <code>exit</code><br><br><b>Example:</b><br><code>Router(config-if)# exit</code>                                    | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 6 | Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).                                               | —                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7 | <code>end</code><br><br><b>Example:</b><br><code>Router(config)# end</code>                                         | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Configuring an eBGP Session Between the Loopbacks

Perform this task to configure an eBGP session between the loopbacks.

**Note**

You need to configure an eBGP session between loopbacks on each directly connected ASBR.

## SUMMARY STEPS

1. `enable`

2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default route-target filter**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family vpv4** [**unicast**]
9. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
11. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                    |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                                | Configures the BGP routing process. <ul style="list-style-type: none"> <li>• The <i>as-number</i> indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul>                                                                                                             |
| Step 4 | <b>no bgp default route-target filter</b><br><br><b>Example:</b><br>Router(config)# no bgp default route-target filter                                                                     | Disables BGP route-target filtering, and enters router configuration mode. <ul style="list-style-type: none"> <li>• All received BGP VPN-IPv4 routes are accepted by the router.</li> </ul>                                                                                                                                                                          |
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20<br>remote-as 100 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>• The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>• The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>• The <i>as-number</i> argument is the autonomous system to which the neighbor belongs.</li> </ul> |

| Command or Action                                                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 6</b></p> <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>disable-connected-check</b></p> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20<br/>disable-connected-check</p>                                                        | <p>Allows peering between loopbacks.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p><b>Step 7</b></p> <p><b>neighbor</b> {<i>ip-address</i>   <i>ipv6-address</i>   <i>peer-group-name</i>} <b>update-source</b> <i>interface-type</i> <i>interface-number</i></p> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20<br/>update-source Loopback 0</p> | <p>Allows BGP sessions in Cisco IOS releases to use any operational interface for TCP connections.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |
| <p><b>Step 8</b></p> <p><b>address-family vpngv4</b> [<b>unicast</b>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family vpngv4</p>                                                                                                                                     | <p>Enters address family configuration mode for configuring routing protocols such as BGP, Routing Information Protocol (RIP), and static routing.</p> <ul style="list-style-type: none"> <li>The <b>vpngv4</b> keyword configures sessions that carry customer VPN-IPv4 prefixes, each of which has been made globally unique by the addition of an 8-byte route distinguisher.</li> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> </ul>                                                                                                                                                                                                                                                                                               |
| <p><b>Step 9</b></p> <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>   <i>ipv6-address</i>} <b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.20.20.20<br/>activate</p>                                                                 | <p>Enables the exchange of information with a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p>                                                                                                                                                                                                                                |

|         | Command or Action                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <pre>neighbor {ip-address   peer-group-name} send-community [both   standard   extended]</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.20.20.20<br/>send-community extended</p> | <p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <b>both</b> keyword specifies that both standard and extended communities will be sent.</li> <li>The <b>standard</b> keyword specifies that only standard communities will be sent.</li> <li>The <b>extended</b> keyword specifies that only extended communities will be sent.</li> </ul> |
| Step 11 | <pre>end</pre> <p><b>Example:</b><br/>Router(config)# end</p>                                                                                                                                        | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Verifying That Load Sharing Occurs Between Loopbacks

Perform this task to verify that load sharing occurs between loopbacks. You need to ensure that the MPLS Label Forwarding Information Base (LFIB) entry for the neighbor route lists the available paths and interfaces.

### SUMMARY STEPS

- enable**
- show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]
- disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                | Purpose                                                                                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                     | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <code>show mpls forwarding-table</code> [network {mask   length}   labels label [-label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]] [vrf vrf-name] [detail]<br><br><b>Example:</b><br>Router# show mpls forwarding-table | Displays the contents of the MPLS LFIB.                                                                           |
| Step 3 | <code>disable</code><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                   | Exits to user EXEC mode.                                                                                          |

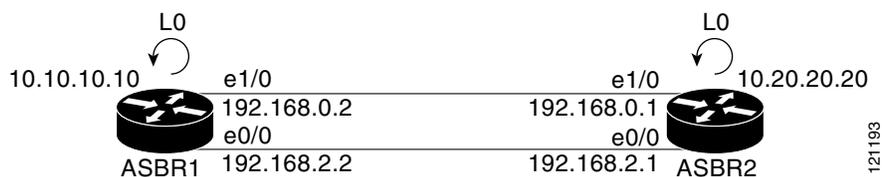
## Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS Using ASBRs to Exchange IPv4 Routes and Labels

The following sections describe how to configure peering of loopback interfaces of directly connected ASBRs to achieve load sharing in an Interautonomous system network:

- [Configuring Loopback Interface Addresses for Directly Connected ASBRs, page 25](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback, page 26](#) (required)
- [Configuring Forwarding on Connecting Loopback Interfaces, page 27](#) (required)
- [Configuring an eBGP Session Between the Loopbacks, page 28](#) (required)
- [Verifying That Load Sharing Occurs Between Loopbacks, page 31](#) (optional)

Figure 4 shows the loopback configuration for directly connected ASBR1 and ASBR2 routers. This configuration is used as the example in the tasks that follow.

**Figure 4** Loopback Interface Configuration for Directly Connected ASBR1 and ASBR2 Routers



121193

## Configuring Loopback Interface Addresses for Directly Connected ASBRs

Perform this task to configure loopback interface addresses.



### Note

Loopback addresses need to be configured for each directly connected ASBR. That is, configure a loopback address for ASBR1 and for ASBR2 in the example (see [Figure 4](#)).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address mask* [**secondary**]
5. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>interface loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 0                                     | Configures a software-only virtual interface that emulates an interface that is always up. <ul style="list-style-type: none"> <li>• The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li> </ul>                                                                                       |
| Step 4 | <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]<br><br><b>Example:</b><br>Router(config-if)# ip address 10.10.10.10<br>255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>• The <i>ip-address</i> argument is the IP address.</li> <li>• The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>• The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                          | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                      |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback

Perform this task to configure /32 static routes to the eBGP neighbor loopback.



### Note

You need to configure /32 static routes on each of the directly connected ASBRs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask {ip-address | interface-type interface-number [ip-address]}*  
[*distance*] [*name*] [**permanent**] [**tag tag**]
4. **end**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|               | Command or Action                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <pre><b>ip route</b> prefix mask {ip-address   interface-type interface-number [ip-address]} [distance] [name] [<b>permanent</b>] [<b>tag</b> tag]</pre> <p><b>Example:</b><br/> Router(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1</p> | Establishes static routes. <ul style="list-style-type: none"> <li>• The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>• The <i>mask</i> argument is the prefix mask for the destination.</li> <li>• The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the specified network.</li> <li>• The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>• The <i>distance</i> argument is an administrative distance.</li> <li>• The <i>name</i> argument applies a name to the specified route.</li> <li>• The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>• The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution through the use of route maps.</li> </ul> |
| <b>Step 4</b> | <pre><b>end</b></pre> <p><b>Example:</b><br/> Router(config)# end</p>                                                                                                                                                                                             | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuring Forwarding on Connecting Loopback Interfaces

Perform this task to configure forwarding on the connecting loopback interfaces.

This task is required for sessions between loopbacks. In the [“Configuring /32 Static Routes to the eBGP Neighbor Loopback”](#) task, Ethernet1/0 and Ethernet0/0 are the connecting interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mpls bgp forwarding**
5. **exit**
6. Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0)
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code>                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <code>interface type slot/port</code><br><br><b>Example:</b><br><code>Router(config)# interface ethernet 1/0</code> | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |
| Step 4 | <code>mpls bgp forwarding</code><br><br><b>Example:</b><br><code>Router(config-if)# mpls bgp forwarding</code>      | Configures BGP to enable MPLS forwarding on connecting interfaces.                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <code>exit</code><br><br><b>Example:</b><br><code>Router(config-if)# exit</code>                                    | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 6 | Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).                                               | —                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7 | <code>end</code><br><br><b>Example:</b><br><code>Router(config)# end</code>                                         | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Configuring an eBGP Session Between the Loopbacks

Perform the following tasks to configure an eBGP session between the loopbacks.

**Note**

You need to configure an eBGP session between loopbacks on each directly connected ASBR.

## SUMMARY STEPS

1. `enable`

2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family ipv4** [**unicast**] **vrf** *vrf-name*
9. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
11. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                                | Configures the BGP routing process, and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul>                                                             |
| Step 4 | <b>bgp log-neighbor-changes</b><br><br><b>Example:</b><br>Router(config-router)# bgp log-neighbor-changes                                                                                  | Enables logging of BGP neighbor resets.                                                                                                                                                                                                                                                                                                                             |
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20<br>remote-as 100 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>• The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>• The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>• The <i>as-number</i> argument is the number of the AS to which the neighbor belongs.</li> </ul> |

| Command or Action                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 6</b></p> <pre><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>disable-connected-check</b></pre> <p><b>Example:</b><br/> Router(config-router)# neighbor 10.20.20.20 disable-connected-check</p>                                                            | <p>Allows peering between loopbacks.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p><b>Step 7</b></p> <pre><b>neighbor</b> {<i>ip-address</i>   <i>ipv6-address</i>   <i>peer-group-name</i>} <b>update-source</b> <i>interface-type</i> <i>interface-number</i></pre> <p><b>Example:</b><br/> Router(config-router)# neighbor 10.20.20.20 update-source Loopback 0</p> | <p>Allows BGP sessions in Cisco IOS releases to use any operational interface for TCP connections.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |
| <p><b>Step 8</b></p> <pre><b>address-family ipv4</b> [<b>unicast</b>] <b>vrf</b> <i>vrf-name</i></pre> <p><b>Example:</b><br/> Router(config-router)# address-family ipv4</p>                                                                                                          | <p>Enters address family configuration mode for configuring routing protocols such as BGP, Routing Information Protocol (RIP), and static routing.</p> <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword configures sessions that carry standard IPv4 address prefixes.</li> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of a VPN routing/forwarding instance (VRF) to associate with submodule commands.</li> </ul>                                                                                                                                                                                                                            |
| <p><b>Step 9</b></p> <pre><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>   <i>ipv6-address</i>} <b>activate</b></pre> <p><b>Example:</b><br/> Router(config-router-af)# neighbor 10.20.20.20 activate</p>                                                                 | <p>Enables the exchange of information with a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p>                                                                                                                                                                                                                              |

|         | Command or Action                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <pre>neighbor {ip-address   peer-group-name} send-community [both   standard   extended]</pre> <p><b>Example:</b><br/> Router(config-router-af)# neighbor 10.20.20.20 send-community extended</p> | <p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>• The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>• The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>• The <b>both</b> keyword specifies that both standard and extended communities will be sent.</li> <li>• The <b>standard</b> keyword specifies that only standard communities will be sent.</li> <li>• The <b>extended</b> keyword specifies that only extended communities will be sent.</li> </ul> |
| Step 11 | <pre>end</pre> <p><b>Example:</b><br/> Router(config)# end</p>                                                                                                                                    | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Verifying That Load Sharing Occurs Between Loopbacks

To verify that load sharing can occur between loopbacks, ensure that the MPLS LFIB entry for the neighbor route lists the available paths and interfaces.

### SUMMARY STEPS

1. **enable**
2. **show mpls forwarding-table** [*network {mask | length}*] | **labels** *label [-label]* | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*] [**vrf** *vrf-name*] [**detail**]
3. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                      | Purpose                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <p><b>show mpls forwarding-table</b> [<i>network {mask   length}</i>]   <b>labels</b> <i>label</i> [<i>-label</i>]   <b>interface</b> <i>interface</i>   <b>next-hop</b> <i>address</i>   <b>lsp-tunnel</b> [<i>tunnel-id</i>] [<i>vrf vrf-name</i>] [<b>detail</b>]</p> <p><b>Example:</b><br/>Router# show mpls forwarding-table</p> | <p>Displays the contents of the MPLS LFIB.</p>                                                                          |
| Step 3 | <p><b>disable</b></p> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                                                                                                                       | <p>Exits to user EXEC mode.</p>                                                                                         |

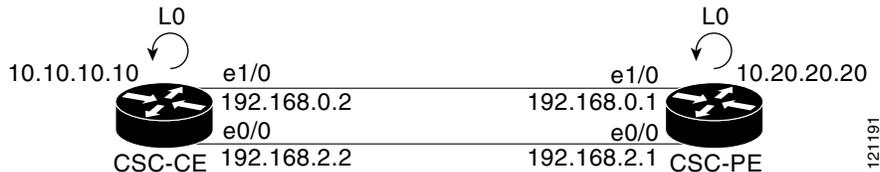
## Configuring Directly Connected Loopback Peering on MPLS VPN Carrier Supporting Carrier

The following sections explain how to load balance CSC traffic by peering loopback interfaces of directly connected CSC-PE and CSC-CE routers:

- [Configuring Loopback Interface Addresses on CSC-PE Routers, page 33](#) (required)
- [Configuring Loopback Interface Addresses for CSC-CE Routers, page 34](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-PE Router, page 35](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-CE Router, page 37](#) (required)
- [Configuring Forwarding on CSC-PE Interfaces That Connect to the CSC-CE Loopback, page 38](#) (required)
- [Configuring Forwarding on CSC-CE Interfaces That Connect to the CSC-PE Loopback, page 40](#) (required)
- [Configuring an eBGP Session Between the CSC-PE Router and the CSC-CE Loopback, page 41](#) (required)
- [Configuring an eBGP Session Between the CSC-CE Router and the CSC-PE Loopback, page 44](#) (required)
- [Verifying That Load Sharing Occurs Between Loopbacks, page 46](#) (optional)

Figure 5 shows the loopback configuration for directly connected CSC-PE and CSC-CE routers. This configuration is used as the example in the tasks that follow.

**Figure 5 Loopback Interface Configuration for Directly Connected CSC-PE and CSC-CE Routers**



121191

**Restrictions**

Load sharing using directly connected loopback peering does not apply to CSC networks that use LDP and an IGP to distribute routes and MPLS labels.

**Configuring Loopback Interface Addresses on CSC-PE Routers**

Perform this task to configure loopback interface addresses on the CSC-PE router.



**Note**

Configuration of a loopback interface address on the CSC-PE router requires the enabling of a VPN VRF. The CSC-CE router loopback interface does not require the enabling of a VRF.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask* [**secondary**]
6. **end**

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                       | <b>Purpose</b>                                                                                                      |
|---------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                   |

|        | Command or Action                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 0                            | Configures a software-only virtual interface that emulates an interface that is always up, and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li> </ul>                                          |
| Step 4 | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1                                | Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                  |
| Step 5 | <b>ip address</b> <i>ip-address mask [secondary]</i><br><br><b>Example:</b><br>Router(config-if)# ip address 10.20.20.20<br>255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                    | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring Loopback Interface Addresses for CSC-CE Routers

Perform this task to configure loopback interface addresses for CSC-CE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address mask [secondary]*
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>interface loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 0                            | Configures a software-only virtual interface that emulates an interface that is always up. <ul style="list-style-type: none"> <li>The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li> </ul>                                                                                   |
| Step 4 | <b>ip address</b> <i>ip-address mask [secondary]</i><br><br><b>Example:</b><br>Router(config-if)# ip address 10.10.10.10<br>255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                 | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-PE Router

Perform the following task to configure /32 static routes to the eBGP neighbor loopback on the CSC-PE router.

## SUMMARY STEPS

- enable**
- configure terminal**
- ip route** *vrf-name prefix mask {ip-address | interface-type interface-number [ip-address]}* [**global**] [*distance*] [*name*] [**permanent**] [**tag tag**]
- end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                                                          | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                                                                                                                                                                                     | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <p><b>ip route vrf vrf-name prefix mask {ip-address   interface-type interface-number [ip-address]} [global] [distance] [name] [permanent] [tag tag]</b></p> <p><b>Example:</b><br/>Router(config)# ip route vrf vpn1 10.10.10.10 255.255.255.255 Ethernet1/0 172.16.0.2</p> <p>Router(config)# ip route vrf vpn1 10.10.10.10 255.255.255.255 Ethernet 0/0 168.192.2.2</p> | <p>Establishes static routes for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name of the VRF for the static route.</li> <li>The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>The <i>mask</i> argument is the prefix mask for the destination.</li> <li>The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the destination network.</li> <li>The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>The <b>global</b> keyword specifies that the given next hop address is in the nonVRF routing table.</li> <li>The <i>distance</i> argument is an administrative distance.</li> <li>The <i>name</i> argument applies a name to the specified route.</li> <li>The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution via route maps.</li> </ul> |
| Step 4 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config)# end</p>                                                                                                                                                                                                                                                                                                           | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-CE Router

Perform the following task to configure /32 static routes to the eBGP neighbor loopback for the CSC-CE router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask* { *ip-address* | *interface-type interface-number* [*ip-address*] } [*distance*] [*name*] [**permanent**] [**tag tag**]
4. **end**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

| Command or Action                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 3</b></p> <pre>ip route prefix mask {ip-address   interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]</pre> <p><b>Example:</b><br/> Router(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1</p> | <p>Establishes static routes.</p> <ul style="list-style-type: none"> <li>• The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>• The <i>mask</i> argument is the prefix mask for the destination.</li> <li>• The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the destination network.</li> <li>• The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>• The <i>distance</i> argument is an administrative distance.</li> <li>• The <i>name</i> argument applies a name to the specified route.</li> <li>• The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>• The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution via route maps.</li> </ul> |
| <p><b>Step 4</b></p> <pre>end</pre> <p><b>Example:</b><br/> Router(config)# end</p>                                                                                                                                                                               | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Configuring Forwarding on CSC-PE Interfaces That Connect to the CSC-CE Loopback

Perform this task to configure forwarding on CSC-PE interfaces that connect to the CSC-CE loopback.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask* [**secondary**]
6. **mpls bgp forwarding**
7. **exit**
8. Repeat Steps 3 through 6 for another connecting interface (Ethernet 0/0).
9. **end**

## DETAILED STEPS—CSC-PE

|        | Command or Action                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                          | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                     | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <p><b>interface</b> <i>type slot/port</i></p> <p><b>Example:</b><br/>Router(config)# interface ethernet 1/0</p>                                            | <p>Configures an interface type and enters interface configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |
| Step 4 | <p><b>ip vrf forwarding</b> <i>vrf-name</i></p> <p><b>Example:</b><br/>Router(config-if)# ip vrf forwarding vpn1</p>                                       | <p>Associates a VRF with an interface or subinterface.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                       |
| Step 5 | <p><b>ip address</b> <i>ip-address mask</i> [<b>secondary</b>]</p> <p><b>Example:</b><br/>Router(config-if)# ip address 172.16.0.1<br/>255.255.255.255</p> | <p>Sets a primary or secondary IP address for an interface.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul>                           |
| Step 6 | <p><b>mpls bgp forwarding</b></p> <p><b>Example:</b><br/>Router(config-if)# mpls bgp forwarding</p>                                                        | <p>Configures BGP to enable MPLS forwarding on connecting interfaces.</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 7 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                                                      | <p>Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |

|        | Command or Action                                                         | Purpose                        |
|--------|---------------------------------------------------------------------------|--------------------------------|
| Step 8 | Repeat Steps 3 through 6 for another connecting interface (Ethernet 0/0). | —                              |
| Step 9 | <code>end</code>                                                          | Exits to privileged EXEC mode. |
|        | <b>Example:</b><br><code>Router(config)# end</code>                       |                                |

## Configuring Forwarding on CSC-CE Interfaces That Connect to the CSC-PE Loopback

Perform this task to configure forwarding on CSC-CE interfaces that connect to the CSC-PE loopback.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `mpls bgp forwarding`
5. `exit`
6. Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).
7. `end`

### DETAILED STEPS

|        | Command or Action                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
|        | <b>Example:</b><br><code>Router&gt; enable</code>                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 2 | <code>configure terminal</code>                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                             |
|        | <b>Example:</b><br><code>Router# configure terminal</code>             |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <code>interface type slot/port</code>                                  | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type</i> argument is the type of interface to be configured.</li> <li>• The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>• The <i>port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |
|        | <b>Example:</b><br><code>Router(config)# interface ethernet 1/0</code> |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|        | Command or Action                                                                           | Purpose                                                            |
|--------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Step 4 | <b>mpls bgp forwarding</b><br><br><b>Example:</b><br>Router(config-if)# mpls bgp forwarding | Configures BGP to enable MPLS forwarding on connecting interfaces. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                               | Exits to global configuration mode.                                |
| Step 6 | Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).                       | —                                                                  |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                    | Exits to privileged EXEC mode.                                     |

## Configuring an eBGP Session Between the CSC-PE Router and the CSC-CE Loopback

Perform this task to configure an eBGP session between the CSC-PE router and the CSC-CE loopback.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family ipv4** [**unicast**] **vrf** *vrf-name*
9. **ip vrf forwarding** *vrf-name*
10. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
11. **neighbor** *ip-address* **send-label**
12. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                              | Configures the BGP routing process. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul>                                                                                                |
| Step 4 | <b>bgp log-neighbor-changes</b><br><br><b>Example:</b><br>Router(config-router)# bgp log-neighbor-changes                                                                         | Enables logging of BGP neighbor resets.                                                                                                                                                                                                                                                                                                                        |
| Step 5 | <b>neighbor {ip-address   peer-group-name}</b><br><b>remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.10.10.10<br>remote-as 100               | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>as-number</i> argument is the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 6 | <b>neighbor {ip-address   peer-group-name}</b><br><b>disable-connected-check</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.10.10.10<br>disable-connected-check | Allows peering between loopbacks. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                            |

| Command or Action                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 7</b></p> <pre><b>neighbor</b> {<i>ip-address</i>   <i>ipv6-address</i>   <i>peer-group-name</i>} <b>update-source</b> <i>interface-type</i> <i>interface-number</i></pre> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.10.10.10<br/>update-source Loopback 0</p> | <p>Allows BGP sessions in Cisco IOS releases to use any operational interface for TCP connections.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |
| <p><b>Step 8</b></p> <pre><b>address-family ipv4</b> [<b>unicast</b>] <b>vrf</b> <i>vrf-name</i></pre> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf<br/>vpn1</p>                                                                                                 | <p>Enters the address family configuration mode for configuring routing protocols such as BGP, Routing Information Protocol (RIP), and static routing.</p> <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword configures sessions that carry standard IPv4 address prefixes.</li> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of a VRF to associate with submode commands.</li> </ul>                                                                                                                                                                                                                                                            |
| <p><b>Step 9</b></p> <pre><b>ip vrf forwarding</b> <i>vrf-name</i></pre> <p><b>Example:</b><br/>Router(config-router-af)# ip vrf forwarding<br/>vpn1</p>                                                                                                                                  | <p>Associates a VRF with an interface or subinterface.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p><b>Step 10</b></p> <pre><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>   <i>ipv6-address</i>} <b>activate</b></pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.10.10.10<br/>activate</p>                                                                | <p>Enables the exchange of information with a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p>                                                                                                                                                                                                                              |

|         | Command or Action                                                                                                                          | Purpose                                                                                                                                                                                                             |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.10.10.10<br>send-label | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> </ul> |
| Step 12 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                   | Exits to privileged EXEC mode.                                                                                                                                                                                      |

## Configuring an eBGP Session Between the CSC-CE Router and the CSC-PE Loopback

Perform this task to configure an eBGP session between the CSC-CE router and the CSC-PE loopback.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family ipv4** [**unicast**] [**vrf** *vrf-name*]
9. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
10. **neighbor** *ip-address* **send-label**
11. **end**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|        | Command or Action                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>router bgp as-number</pre> <p><b>Example:</b><br/>Router(config)# router bgp 200 </p>                                                                                                                       | <p>Configures the BGP routing process.</p> <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 4 | <pre>bgp log-neighbor-changes</pre> <p><b>Example:</b><br/>Router(config-router)# bgp log-neighbor-changes </p>                                                                                                  | <p>Enables logging of BGP neighbor resets.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 5 | <pre>neighbor {ip-address   peer-group-name} remote-as as-number</pre> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20 remote-as 100 </p>                                                     | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>as-number</i> argument is the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 6 | <pre>neighbor {ip-address   peer-group-name} disable-connected-check</pre> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20 disable-connected-check </p>                                       | <p>Allows peering between loopbacks.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 7 | <pre>neighbor {ip-address   ipv6-address   peer-group-name} update-source interface-type interface-number</pre> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20 update-source Loopback 0 </p> | <p>Allows BGP sessions in Cisco IOS releases to use any operational interface for TCP connections.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |

|         | Command or Action                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <p><b>address-family ipv4</b> [<b>unicast</b>] [<b>vrf vrf-name</b>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4</p>                                               | <p>Enters the address family configuration mode for configuring routing protocols such as BGP, RIP, and static routing.</p> <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword configures sessions that carry standard IPv4 address prefixes.</li> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of a VRF to associate with submode commands.</li> </ul>                                                                     |
| Step 9  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>   <i>ipv6-address</i>} <b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.20.20.20 activate</p> | <p>Enables the exchange of information with a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> |
| Step 10 | <p><b>neighbor ip-address send-label</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.20.20.20 send-label</p>                                                            | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> </ul>                                                                                                                                                                                                                                                                                                   |
| Step 11 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config)# end</p>                                                                                                                             | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Verifying That Load Sharing Occurs Between Loopbacks

To verify that load sharing occurs between loopbacks, ensure that the MPLS LFIB entry for the neighbor route lists the available paths and interfaces.

### SUMMARY STEPS

- enable**
- show mpls forwarding-table** [**vrf vrf-name**] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
- disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                            | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show mpls forwarding-table</b> [ <b>vrf</b> <i>vrf-name</i> ]<br>[{ <i>network</i> { <i>mask</i>   <i>length</i> }   <b>labels</b> <i>label</i><br>[- <i>label</i> ]   <b>interface</b> <i>interface</i>   <b>next-hop</b><br><i>address</i>   <b>lsp-tunnel</b> [ <i>tunnel-id</i> ]}] [ <b>detail</b> ] | Displays the contents of the MPLS LFIB.                                                                          |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                                                                     | Exits to user EXEC mode.                                                                                         |

## Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic | Document Title                                       |
|---------------|------------------------------------------------------|
| MPLS          | <a href="#">Multiprotocol Label Switching (MPLS)</a> |
| BGP           | <a href="#">Configuring BGP</a>                      |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                             |
|----------|-------------------------------------------------------------------|
| RFC 1164 | <i>Application of the Border Gateway Protocol in the Internet</i> |
| RFC 1171 | <i>A Border Gateway Protocol 4</i>                                |
| RFC 1700 | <i>Assigned Numbers</i>                                           |
| RFC 1966 | <i>BGP Route Reflection: An Alternative to Full Mesh IBGP</i>     |
| RFC 2283 | <i>Multiprotocol Extensions for BGP-4</i>                         |
| RFC 2373 | <i>IP Version 6 Addressing Architecture</i>                       |
| RFC 2547 | <i>BGP/MPLS VPNs</i>                                              |
| RFC 2842 | <i>Capabilities Advertisement with BGP-4</i>                      |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>                         |
| RFC 3107 | <i>Carrying Label Information in BGP-4</i>                        |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for Load Sharing MPLS VPN Traffic

[Table 1](#) lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

**Note**

**Table 1** lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Load Sharing MPLS VPN Traffic

| Feature Name                                                     | Releases                           | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Load Balancing Support for Inter-AS and CSC VPNs        | 12.0(29)S<br>12.4(20)T             | <p>This feature allows MPLS VPN Inter-AS and MPLS VPN CSC networks to load share traffic between adjacent LSRs that are connected by multiple links. The LSRs can be a pair of ASBRs or a CSC-PE and a CSC-CE. Using directly connected loopback peering allows load sharing at the IGP level, so more than one BGP session is not needed between the LSRs. No other label distribution mechanism is needed between the adjacent LSRs than BGP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Load Sharing Using Directly Connected Loopback Peering, page 6</a></li> <li>• <a href="#">Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS using ASBRs to Exchange VPN-IPv4 Addresses, page 16</a></li> </ul> |
| BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN | 12.2(4)T<br>12.2(14)S<br>12.0(24)S | <p>This feature allows multihomed autonomous systems and PE routers to be configured to distribute traffic across both external BGP (eBGP) and internal BGP (iBGP) paths.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Multipath for eBGP and iBGP, page 4</a></li> <li>• <a href="#">Configuring BGP Multipath Load Sharing for eBGP and iBGP, page 7</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                       |

Table 1 Feature Information for Load Sharing MPLS VPN Traffic (continued)

| Feature Name                | Releases              | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iBGP Multipath Load Sharing | 12.2(2)T<br>12.2(14)S | This feature enables the BGP speaking router to select multiple iBGP paths as the best paths to a destination.<br><br>The following section provides information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Internal BGP Multipath Load Sharing, page 4</a></li> </ul>                                                                                                                                                                                                                                                                           |
| eBGP Multipath              | 12.0(27)S             | This feature installs multiple paths in the IP routing table when the eBGP paths are learned from a neighboring Autonomous System (AS), instead of picking one best path.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">eBGP Multipath Load Sharing, page 6</a></li> <li>• <a href="#">Configuring eBGP Multipath Load Sharing with MPLS VPN Inter-AS, page 9</a></li> <li>• <a href="#">Configuring eBGP Multipath Load Sharing with MPLS VPN Carrier Supporting Carrier, page 11</a></li> </ul> |

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, 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. (0805R)

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.

© 2005–2008 Cisco Systems, Inc. All rights reserved.



# Dialing to Destinations with the Same IP Address for MPLS VPNs

---

The dialer software in Cisco IOS prior to Release 12.2(8)T had no way to dial two different destinations with the same IP address. More specifically, in networks where a network access server (NAS) supports dialing clients with overlapping addresses, dial-out attempts fail. This module explains how to dial to more than one destination with the same IP address.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Dialing to Destinations with the Same IP Address” section on page 14](#).

## Contents

- [Prerequisites for Dialing to Destinations with the Same IP Address, page 2](#)
- [Restrictions for Dialing to Destinations with the Same IP Address, page 2](#)
- [Information About Dialing to Destinations with the Same IP Address, page 4](#)
- [How to Enable Dialing to Destinations with the Same IP Address, page 5](#)
- [Configuration Examples for Dialing to Destinations with the Same IP Address, page 7](#)
- [Additional References, page 12](#)
- [Feature Information for Dialing to Destinations with the Same IP Address, page 14](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for Dialing to Destinations with the Same IP Address

Before configuring this feature, you should understand how to configure the following network features:

- Virtual profiles with two-way AAA authentication
- MPLS VPNs

Refer to the documents listed in the [“Additional References”](#) section for information about configuring these features.

The Dialing to Destinations with the Same IP Address feature is supported on the following Cisco router and access server platforms:

- Cisco 1600 series
- Cisco 1720
- Cisco 1721
- Cisco 1750
- Cisco 1751
- Cisco 3600 series
- Cisco 3631
- Cisco 3725
- Cisco 3745
- Cisco 7200 series
- Cisco 7500 series
- Cisco 802
- Cisco 820
- Cisco 828
- Cisco uBR7200

# Restrictions for Dialing to Destinations with the Same IP Address

When configuring static routes in an MPLS or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.xT, 12.xM, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later. Use the following guidelines when configuring static routes.

## Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in MPLS environment:

```
ip route destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

#### Unsupported Static Routes in an MPLS Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

```
ip route destination-prefix mask next-hop1
ip route destination-prefix mask next-hop2
```

Use the *interface* and *next-hop* arguments when specifying static routes.

#### Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop and interface are in the same VRF:

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask* **interface1 next-hop1**  
**ip route vrf** *vrf-name destination-prefix mask* **interface2 next-hop2**

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet Gateway.

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*  
(This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

#### Unsupported Static Routes in an MPLS VPN Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

```
ip route vrf destination-prefix mask next-hop-address global
```

The following **ip route** commands are not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

```
ip route vrf destination-prefix mask next-hop1 global
ip route vrf destination-prefix mask next-hop2 global
```

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

```
ip route vrf vrf-name destination-prefix mask next-hop1
ip route vrf vrf-name destination-prefix mask next-hop2
```

#### Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table on the CE side. For example, the following command is supported when the destination-prefix is the CE router's loopback address, as in EBGp multihop cases.

```
ip route vrf vrf-name destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static non-recursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 nexthop1
ip route destination-prefix mask interface2 nexthop2
```

## Information About Dialing to Destinations with the Same IP Address

Before configuring this feature, you should understand the following concepts:

- [Introduction to Dialing to Destinations with the Same IP Address, page 4](#)
- [Benefits of this Feature, page 4](#)

### Introduction to Dialing to Destinations with the Same IP Address

The Cisco IOS dialer software can distinguish between two destinations with the same IP address using information stored in the VRF. This capability is provided to the dialer software by two existing Cisco IOS commands, **dialer map** and **ip route**, which have been enhanced to include VPN routing and forwarding (VRF) information.

In previous Cisco IOS releases, the dialer software obtained the telephone number for dial-out based on the destination IP address configured in the **dialer map** command. Now, the enhanced **dialer map** command supplies the name of the VRF so that the telephone number to be dialed is based on the VRF name and the destination IP address. The VRF is identified based on the incoming interface of the packet, and is used with the destination IP address defined in the **dialer map** command to determine the telephone number to be dialed.

The **ip route** configuration command also includes the VRF information. When a packet arrives in an incoming interface that belongs to a particular VRF, only those **ip route** commands that correspond to that particular VRF are used to determine the destination interface.

### Benefits of this Feature

This feature allows the dialer software to dial out in an MPLS-based VPN. The MPLS VPN model simplifies network routing. For example, rather than needing to manage routing over a complex virtual network backbone composed of many virtual circuits, an MPLS VPN user can employ the backbone of the service provider as the default route in communicating with all other VPN sites.

This default route capability allows several sites to transparently interconnect through the service provider network. One service provider network can support several different IP VPNs, each of which appears to its users as a separate, private network. Within a VPN, each site can send IP packets to any other site in the same VPN, because each VPN is associated with one or more VRFs. The VRF is a key element in the VPN technology, because it maintains the routing information that defines a customer VPN site.

## How to Enable Dialing to Destinations with the Same IP Address

This section includes the following procedures:

- [Mapping the VRF and Next-Hop Address to a Dial String, page 5](#) (required)
- [Verifying the Configuration, page 6](#) (optional)

### Mapping the VRF and Next-Hop Address to a Dial String

Use the following procedure to map a VRF and next-hop address combination to a dial string and thereby allow the dialer software to be VRF-aware for an MPLS VPN.

#### Prerequisites

These commands are only part of the required configuration and show how to map a VRF and next-hop address combination to a dial string. Refer to the documents listed in the “[Additional References](#)” section and the example in the “[Configuration Examples for Dialing to Destinations with the Same IP Address](#)” section for details on where to include these commands in the network configuration.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dialer** *number*
4. **dialer map ip** *protocol-next-hop-address* **vrf** *vrf-name* **name** *host-name dial-string*
5. **end**
6. **ip route vrf** *vrf-name* *ip-address mask interface-type interface-number*

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                                                                                                                | <b>Purpose</b>                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                     |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                          | Enters global configuration mode.                                                                                                    |
| <b>Step 3</b> | <b>interface dialer</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface dialer 1                                                                                                      | Enters interface configuration mode and begins dialer configuration.                                                                 |
| <b>Step 4</b> | <b>dialer map ip</b> <i>protocol-next-hop-address vrf vrf-name name host-name dial-string</i><br><br><b>Example:</b><br>Router(config-if)# dialer map ip 60.0.0.12 vrf yellow name rubbertree02 5552171 | Maps a VRF and next-hop address combination to a dial string (telephone number).                                                     |
| <b>Step 5</b> | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                                                                             | (Optional) Exits interface configuration mode.                                                                                       |
| <b>Step 6</b> | <b>ip route vrf</b> <i>vrf-name ip-address mask interface-type interface-number</i><br><br><b>Example:</b><br>Router(config)# ip route vrf blue 10.0.0.1 255.255.255.255 Dialer0                        | Configures a VRF and next hop address combination that points to the interface where the dialer software should make the connection. |

**Verifying the Configuration**

To verify the configuration, use the following procedure.

**SUMMARY STEPS**

1. ping
2. show adjacency

**DETAILED STEPS****Step 1 ping**

Use this command on the customer edge NAS to place a call to a peer. The expected result is that the NAS successfully dials out to that peer.

**Step 2 show adjacency**

Use this command if the call fails to check Cisco Express Forwarding (CEF) adjacency table information.

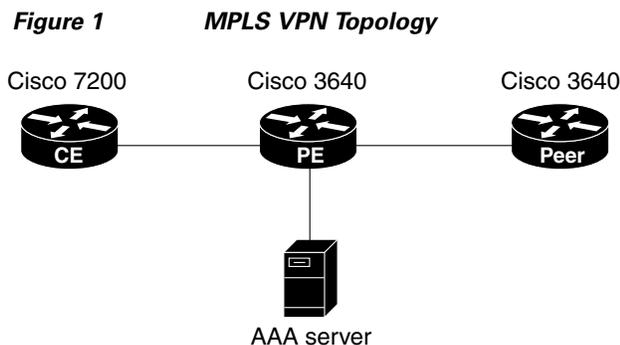
## Troubleshooting Tips

If you encounter problems with the feature, use the following **debug** privileged EXEC commands on the NAS to help you determine where the problem lies:

- **debug aaa authentication**
- **debug aaa authorization**
- **debug dialer**
- **debug ppp authentication**
- **debug ppp negotiation**
- **debug radius**

# Configuration Examples for Dialing to Destinations with the Same IP Address

This section provides a configuration example of the feature for a simple network topology shown in [Figure 1](#).

**Note**

The network addresses and telephone numbers used in the following configuration are examples only and will not work in an actual network configuration.

### Customer Edge (CE) Router

```

!
hostname oaktree02
enable secret 5 !1!35Fg$Ep4.D8JGpg7rKxQa49BF9/
!
ip subnet-zero
no ip domain-lookup
!
controller T1 5/0
!

```

```
controller T1 5/1
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
!
interface Ethernet1/0
 ip address 10.0.58.11 255.255.255.0
 no ip mroute-cache
 half-duplex
!
interface Ethernet1/1
 ip address 50.0.0.2 255.0.0.0
 no ip mroute-cache
 half-duplex
!
interface Ethernet1/2
 no ip address
 no ip mroute-cache
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 no ip mroute-cache
 shutdown
 half-duplex
!
interface Serial2/0
 no ip address
 no ip mroute-cache
 shutdown
 no fair-queue
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
interface FastEthernet4/0
 no ip address
```

```

no ip mroute-cache
shutdown
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.58.1
ip route 60.0.0.0 255.0.0.0 50.0.0.1
no ip http server
!
!
snmp-server manager
banner motd ^C AV-8B OAKTREE^C
alias exec r sh run
!
line con 0
 exec-timeout 0 0
line aux 0
 login
line vty 0 4
 no login
!
end

```

### Provider Edge (PE) Router

```

hostname pinetree02
!
aaa new-model
!
!
aaa authentication login con-log none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa session-id common
enable secret 5 $1$7KlA$xpC814dJJCZogbzZvGUtF1/
!
username rubbertree02 password 0 Hello
ip subnet-zero
!
no ip domain-lookup
!
ip vrf yellow
 rd 100:1
ip cef
virtual-profile aaa
isdn switch-type primary-5ess
!
controller T1 3/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3/1
 framing esf
 linecode b8zs
!
controller T1 3/2
 framing esf
 linecode b8zs
!
controller T1 3/3
 framing esf
 linecode b8zs

```

```

!
controller T1 3/4
 framing esf
 linecode b8zs
!
controller T1 3/5
 framing esf
 linecode b8zs
!
controller T1 3/6
 framing esf
 linecode b8zs
!
controller T1 3/7
 framing esf
 linecode b8zs
!
interface Loopback0
 ip vrf forwarding yellow
 ip address 70.0.0.1 255.0.0.0
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet2/0
 ip address 10.0.58.3 255.255.255.0
 duplex full
!
interface Ethernet2/1
 ip vrf forwarding yellow
 ip address 50.0.0.1 255.0.0.0
 duplex half
!
interface Ethernet2/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet2/3
 no ip address
 shutdown
 duplex half
!
interface Serial3/0:23
 description phone# 555-3123
 no ip address
 encapsulation ppp
 dialer rotary-group 0
 dialer-group 1
 isdn switch-type primary-5ess
 ppp authentication chap
!
interface Serial4/0
 no ip address
 shutdown
 no fair-queue
!
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer in-band
 dialer map ip 60.0.0.12 vrf yellow name rubbertree02 5552171

```

```

dialer map ip 60.0.0.2 5552172
dialer-group 1
ppp authentication chap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.58.1
ip route 60.0.0.2 255.255.255.255 Dialer0
ip route vrf yellow 60.0.0.0 255.0.0.0 Dialer0 permanent
no ip http server
ip pim bidir-enable
!
ip director cache time 60
dialer-list 1 protocol ip permit
!
radius-server host 172.19.192.89 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
shutdown
!
banner motd ^C F/A-18 PINETREE ^C
!
line con 0
exec-timeout 0 0
login authentication con-log

line aux 0
line vty 5 15
!
end

```

### Peer Router

```

hostname rubbertree02
!
logging buffered 32000 debugging
enable secret 5 1RCKC$scgtdlaDzjSyUVai7KK5Q.
enable password Windy
!
username pinetree02 password 0 Hello
!
ip subnet-zero
no ip domain-lookup
!
isdn switch-type basic-5ess
!
interface Ethernet0
ip address 10.0.58.9 255.255.255.0
no ip route-cache
!
interface BRI0
description phone# 555-2171
ip address 60.0.0.12 255.0.0.0
encapsulation ppp
no ip route-cache
dialer map ip 60.0.0.11 5553123
dialer map ip 60.0.0.2 5552172

```

```

dialer-group 1
 isdn switch-type basic-5ess
 isdn fast-rollover-delay 45
!
ip default-gateway 10.0.58.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.58.1
ip route 50.0.0.0 255.0.0.0 70.0.0.1
no ip http server
!
dialer-list 1 protocol ip permit
no cdp run
banner motd ^C F-4B RUBBERTREE^C
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password Windy
 login
!
end

```

### AAA Server User File

```
[aaa-serv]/usr/testing/bin> ./radiusd_1.16 -d . -a .-x
```

```

greentree-16 Password = "Hello", Expiration = "Dec 31 2005"
 Service-Type = Framed-User,
 Framed-Protocol = PPP
 cisco-avpair = "lcp:interface-config=ip vrf forwarding yellow \nip
unnumbered Loopback0"

```

## Additional References

The following sections provide references related to MPLS VPNs.

### Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                      |
|----------|------------------------------------------------------------|
| RFC 1164 | Application of the Border Gateway Protocol in the Internet |
| RFC 1171 | A Border Gateway Protocol 4                                |
| RFC 1700 | Assigned Numbers                                           |
| RFC 1966 | BGP Route Reflection: An Alternative to Full Mesh IBGP     |
| RFC 2283 | Multiprotocol Extensions for BGP-4                         |
| RFC 2547 | BGP/MPLS VPNs                                              |
| RFC 2842 | Capabilities Advertisement with BGP-4                      |
| RFC 2858 | Multiprotocol Extensions for BGP-4                         |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Dialing to Destinations with the Same IP Address

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Dialing to Destinations with the Same IP Address

| Feature Name                       | Releases | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dialer Map VRF-Aware for MPLS VPNs | 12.2(8)T | <p>The Cisco IOS dialer software is "VRF-aware for an MPLS VPN," which means that it can distinguish between two destinations with the same IP address using information stored in the VRF.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Introduction to Dialing to Destinations with the Same IP Address, page 4</a></li> <li>• <a href="#">How to Enable Dialing to Destinations with the Same IP Address, page 5</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# Configuring Scalable Hub-and-Spoke MPLS VPNs

---

This module explains how to ensure that virtual private network (VPN) clients that connect to the same provider edge (PE) router at the edge of the Multiprotocol (MPLS) Virtual Private Network (VPN) use the hub site. This feature prevents the VPN clients from communicating directly with each other, bypassing the hub site. This feature also provides scalable hub-and-spoke connectivity for subscribers of an MPLS VPN service by removing the requirement of one VRF per spoke.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for Configuring Scalable Hub-and-Spoke MPLS VPNs” section on page 16.](#)

## Contents

- [Prerequisites for Configuring Scalable Hub-and-Spoke MPLS VPNs, page 2](#)
- [Restrictions for Configuring Scalable Hub-and-Spoke MPLS VPNs, page 2](#)
- [Information about Configuring Scalable Hub-and-Spoke MPLS VPNs, page 2](#)
- [How to Ensure that MPLS VPN Clients Use the Hub PE Router, page 4](#)
- [Configuration Examples for Configuring Scalable Hub-and-Spoke MPLS VPNs, page 9](#)
- [Additional References, page 14](#)
- [Feature Information for Configuring Scalable Hub-and-Spoke MPLS VPNs, page 16](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Configuring Scalable Hub-and-Spoke MPLS VPNs

You must have a working MPLS core network.

## Restrictions for Configuring Scalable Hub-and-Spoke MPLS VPNs

- In both the upstream and downstream VRFs, routing protocols are not supported on interfaces configured with this feature. Interfaces that are not configured with this feature, however, do not have this restriction for the upstream or downstream VRFs.
- You can configure this feature only on virtual access interfaces (VAIs) and virtual template interfaces (VTIs).
- Only unnumbered interfaces are supported.
- Multicast is not supported on interfaces configured for hub-and-spoke MPLS VPNs.

## Information about Configuring Scalable Hub-and-Spoke MPLS VPNs

To configure this feature, you need to understand the following concepts:

- [Overview, page 2](#)
- [Upstream and Downstream VRFs, page 3](#)
- [Reverse Path Forwarding Check, page 3](#)

## Overview

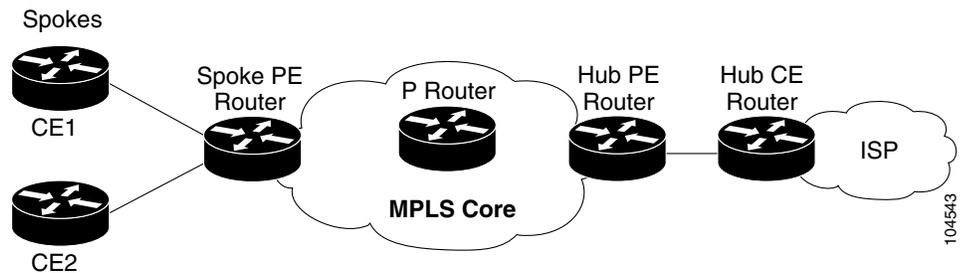
This feature prevents local connectivity between subscribers at the spoke provider edge (PE) router and ensures that a hub site provides subscriber connectivity. Any sites that connect to the same PE router must forward intersite traffic using the hub site. This ensures that the routing done at the spoke site moves from the access-side interface to the network-side interface or from the network-side interface to the access-side interface, but never from the access-side interface to the access-side interface.

This feature prevents situations where the PE router locally switches the spokes without passing the traffic through the hub site. This prevents subscribers from directly connecting to each other.

This feature eases configuration by removing the requirement of one VRF per spoke. In prior releases, when spokes connected to the same PE router, each spoke was configured in a separate VRF to ensure that the traffic between the spokes traversed the central link between the wholesale service provider and the ISP. However, this solution was not scalable. When many spokes connected to the same PE router, configuration of VRFs for each spoke became quite complex and greatly increased memory usage. This was especially true in large-scale environments that supported high-density remote access to Layer 3 VPNs.

[Figure 2](#) shows a sample hub-and-spoke topology.

**Figure 2** *Hub-and-Spoke Topology*



## Upstream and Downstream VRFs

This feature uses two unidirectional VRFs to forward IP traffic between the spokes and the hub PE router:

- The upstream VRF forwards the IP traffic from the spokes toward the hub PE router. This VRF typically contains only a default route but might also contain summary routes and multiple default routes. The default route points to the interface on the hub PE router that connects to the upstream ISP. The router dynamically learns about the default route from the routing updates that the hub PE router or home gateway sends. The upstream VRF also contains the VAIs that connect the spokes, but it contains no other local interfaces.
- The downstream VRF forwards traffic from the hub PE router back to the spokes. This VRF contains Point-to-Point Protocol (PPP) peer routes for the spokes and per-user static routes received from the Authentication, Authorization, and Accounting (AAA) server. It also contains the routes imported from the hub PE router.

The router redistributes routes from the downstream VRF into Multiprotocol Border Gateway Protocol (MP-BGP). The spoke PE router typically advertises a summary route across the MPLS core for the connected spokes. The VRF configured on the hub PE router imports the advertised summary route.

## Reverse Path Forwarding Check

The unicast Reverse Path Forwarding (RPF) check ensures that an IP packet that enters a router uses the correct inbound interface. This feature supports unicast RPF check on the spoke-side interfaces. Because different VRFs are used for downstream and upstream forwarding, the RPF mechanism ensures that source address checks occur in the downstream VRF.

# How to Ensure that MPLS VPN Clients Use the Hub PE Router

This section contains the following procedures:

- [Configuring the Upstream and Downstream VRFs on the PE Router or the Spoke PE Router, page 4](#) (required)
- [Associating VRFs, page 5](#) (required)
- [Configuring the Downstream VRF for an AAA Server, page 6](#) (optional)
- [Verifying the Configuration, page 7](#) (optional)

## Configuring the Upstream and Downstream VRFs on the PE Router or the Spoke PE Router

To configure the upstream and downstream VRFs on the PE router or on the spoke PE router, use the following procedure.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **exit**

### DETAILED STEPS

|        | Command or Action                                                                | Purpose                                                                                                            |
|--------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal   | Enters global configuration mode.                                                                                  |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# ip vrf U | Enters VRF configuration mode and defines the VRF instance by assigning a VRF name.                                |

|        | Command or Action                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <pre>rd route-distinguisher</pre> <p><b>Example:</b><br/>Router(config-vrf)# rd 1:0</p>                                                            | Creates routing and forwarding tables.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 5 | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf)# route-target import 1:0</p> | Creates a list of import and export route target communities for the specified VRF. <ul style="list-style-type: none"> <li>• The <b>import</b> keyword is required to create an upstream VRF. The upstream VRF is used to import the default route from the hub PE router.</li> <li>• The <b>export</b> keyword is required to create a downstream VRF. The downstream VRF is used to export the routes of all subscribers of a given service that the VRF serves.</li> </ul> |
| Step 6 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-vrf)# exit</p>                                                                                | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Associating VRFs

The virtual template interface is used to create and configure a virtual access interface (VAI). After you define and configure the VRFs on the PE routers, associate each VRF with the following:

- Interface or subinterface
- Virtual template interface

To associate a VRF, enter the following commands on the PE router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip vrf forwarding** *vrf-name1* [**downstream** *vrf-name2*]
5. **ip unnumbered** *type number*
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>interface virtual-template</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface virtual-template 1                                            | Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces. Enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                    |
| Step 4 | <b>ip vrf forwarding</b> <i>vrf-name1</i> [ <b>downstream</b> <i>vrf-name2</i> ]<br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1 downstream D | Associates a virtual template interface with the VRF you specify. <ul style="list-style-type: none"> <li>The <i>vrf-name1</i> argument is the name of the VRF associated with the virtual template interface.</li> <li>The <i>vrf-name2</i> argument is the name of the downstream VRF into which the PPP peer route and all of the per-user routes from the AAA server are installed. If an AAA server is used, it provides the VRF membership; you do not need to configure the VRF members on the virtual templates.</li> </ul> |
| Step 5 | <b>ip unnumbered</b> <i>type number</i><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered Loopback1                                                      | Enables IP processing on an interface without assigning an explicit IP address to the interface.<br><br>The <i>type</i> and <i>number</i> arguments are the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.                                                                                                                                                                                                                                        |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                     | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Configuring the Downstream VRF for an AAA Server

To configure the downstream VRF for an AAA server, enter the following Cisco attribute value:

**lcp:interface-config=ip vrf forwarding U downstream D**

For more information about configuring a RADIUS server, see [Configuring Virtual Template Interfaces](#).

## Verifying the Configuration

To verify the configuration, perform the following steps.

### SUMMARY STEPS

1. `show ip vrf [brief | detail | interfaces | id] [vrf-name] [output-modifiers]`
2. `show ip route vrf vrf-name`
3. `show running-config [interface type number]`

### DETAILED STEPS

#### Step 1 `show ip vrf [brief | detail | interfaces | id] [vrf-name] [output-modifiers]`

Use this command to display information about all of the VRFs configured on the router, including the downstream VRF for each associated VAI.

```
Router# show ip vrf

Name Default RD Interface
D 2:0 Loopback2
 Virtual-Access3 [D]
 Virtual-Access4 [D]

U 2:1 Virtual-Access3
 Virtual-Access4
```

#### `show ip vrf detail vrf-name`

Use this command to display detailed information about the VRF you specify, including all of the VAIs associated with the VRF.

If you do not specify a value for *vrf-name*, detailed information about all of the VRFs configured on the router appears, including all of the VAIs associated with each VRF.

The following example shows how to display detailed information for the VRF called vrf1.

```
Router# show ip vrf detail vrf1

VRF D; default RD 2:0; default VPNID <not set>
 Interfaces:
 Loopback2 Virtual-Access3 [D] Virtual-Access4 [D]
 Connected addresses are not in global routing table
 Export VPN route-target communities
 RT:2:0
 Import VPN route-target communities
 RT:2:1
 No import route-map
 No export route-map
VRF U; default RD 2:1; default VPNID <not set>
 Interfaces:
 Virtual-Access3 Virtual-Access4
 Connected addresses are not in global routing table
 No Export VPN route-target communities
 Import VPN route-target communities
 RT:2:1
 No import route-map
 No export route-map
```

#### Step 2 `show ip route vrf vrf-name`

Use this command to display the IP routing table for the VRF you specify, and information about the per-user static routes installed in the downstream VRF.

The following example shows how to display the routing table for the downstream VRF named D.

```
Router# show ip route vrf D
```

```
Routing Table: D
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```

 2.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
U 2.0.0.2/32 [1/0] via 2.8.1.1
S 2.0.0.0/8 is directly connected, Null0
U 2.0.0.5/32 [1/0] via 2.8.1.2
C 2.8.1.2/32 is directly connected, Virtual-Access4
C 2.8.1.1/32 is directly connected, Virtual-Access3
```

The following example shows how to display the routing table for the upstream VRF named U.

```
Router# show ip route vrf U
```

```
Routing Table: U
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route
```

```
Gateway of last resort is 100.0.0.20 to network 0.0.0.0
```

```

 2.0.0.0/32 is subnetted, 1 subnets
C 2.0.0.8 is directly connected, Loopback2
B* 0.0.0.0/0 [200/0] via 100.0.0.20, 1w5d
```

**Step 3** `show running-config [interface type number]`

Use this command to display information about the virtual access interface you specify, including information about the upstream and downstream VRFs.

The following example shows how to display information about the interface named virtual-access 3.

```
Router# show running-config interface virtual-access 3

Building configuration...

Current configuration : 92 bytes
!
interface Virtual-Access3
 ip vrf forwarding U downstream D
 ip unnumbered Loopback2
end
```

The following example shows how to display information about the interface named virtual-access 4.

```
Router# show running-config interface virtual-access 4

Building configuration...

Current configuration : 92 bytes
!
interface Virtual-Access4
 ip vrf forwarding U downstream D
 ip unnumbered Loopback2
end
```

---

## Configuration Examples for Configuring Scalable Hub-and-Spoke MPLS VPNs

This section provides the following configuration examples:

- [Configuring the Upstream and Downstream VRFs on the PE Router and the Spoke PE Router: Example, page 10](#)
- [Associating VRFs: Example, page 10](#)
- [Configuring Scalable Hub-and-Spoke MPLS VPNs—Basic Configuration: Example, page 11](#)
- [Configuring Scalable Hub-and-Spoke MPLS VPNs: Example, page 12](#)

## Configuring the Upstream and Downstream VRFs on the PE Router and the Spoke PE Router: Example

The following example configures an upstream VRF named U:

```
Router> enable
Router# configure terminal
Router(config)# ip vrf U
Router(config-vrf)# rd 1:0
Router(config-vrf)# route-target import 1:0
```

The following example configures a downstream VRF named D:

```
Router> enable
Router# configure terminal
Router(config)# ip vrf D
Router(config-vrf)# rd 1:8
Router(config-vrf)# route-target export 1:100
```

## Associating VRFs: Example

The following example associates the VRF named U with the virtual-template 1 interface and specifies the downstream VRF named D:

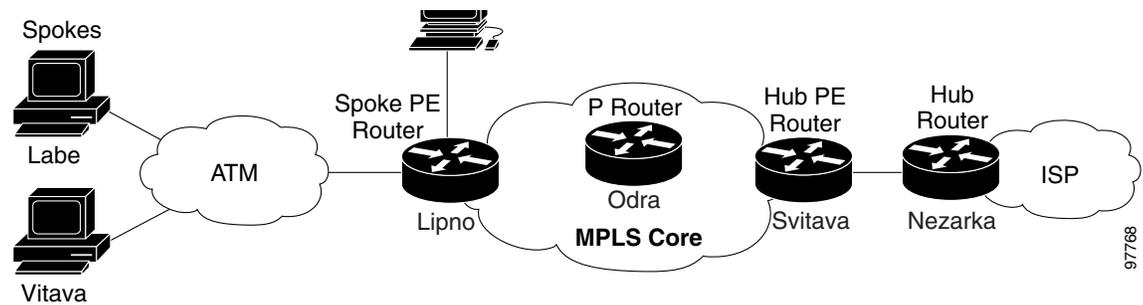
```
Router> enable
Router# configure terminal
Router(config)# interface virtual-template 1
Router(config-if)# ip vrf forwarding U downstream D
Router(config-if)# ip unnumbered Loopback1
```

## Configuring Scalable Hub-and-Spoke MPLS VPNs—Basic Configuration: Example

In this example, local authentication is used; that is, the RADIUS server is not used.

This example uses the hub-and-spoke topology shown in [Figure 3](#).

**Figure 3** Sample Topology



```

ip vrf D
 rd 1:8
 route-target export 1:100
!
ip vrf U
 rd 1:0
 route-target import 1:0
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
 protocol pppoe
 virtual-template 1
!
interface Loopback2
 ip vrf forwarding U
 ip address 2.0.0.8 255.255.255.255
!
interface ATM2/0
 description Mze ATM3/1/2
 no ip address
 no atm ilmi-keepalive
 pvc 0/16 ilmi
!
 pvc 3/100
 protocol pppoe
!
 pvc 3/101
 protocol pppoe
!
interface Virtual-Templat1
 ip vrf forwarding U downstream D
 ip unnumbered Loopback2
 peer default ip address pool U-pool
 ppp authentication chap

```

## Configuring Scalable Hub-and-Spoke MPLS VPNs: Example

The following example shows how to connect two Point-to-Point Protocol over Ethernet (PPPoE) clients to a single VRF pair on the spoke PE router named Lipno. Although both PPPoE clients are configured in the same VRF, all communication occurs using the hub PE router. Half-duplex VRFs are configured on the spoke PE. The client configuration is downloaded to the spoke PE from the RADIUS server.

This example uses the hub-and-spoke topology shown in [Figure 3](#).



### Note

The wholesale provider can forward the user authentication request to the corresponding ISP. If the ISP authenticates the user, the wholesale provider appends the VRF information to the request that goes back to the PE router.

```

aaa new-model
!
aaa group server radius R
 server 22.0.20.26 auth-port 1812 acct-port 1813
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
ip vrf D
 description Downstream VRF - to spokes
 rd 1:8
 route-target export 1:100
!
ip vrf U
 description Upstream VRF - to hub
 rd 1:0
 route-target import 1:0
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
 protocol pppoe
 virtual-template 1
!
interface Loopback2
 ip vrf forwarding U
 ip address 2.0.0.8 255.255.255.255
!
interface ATM2/0
 pvc 3/100
 protocol pppoe
!
pvc 3/101
 protocol pppoe
!
interface virtual-template 1
 no ip address
 ppp authentication chap
!
router bgp 1
 no synchronization
 neighbor 100.0.0.34 remote-as 1
 neighbor 100.0.0.34 update-source Loopback0
 no auto-summary
!

```

```
address-family vpnv4
 neighbor 100.0.0.34 activate
 neighbor 100.0.0.34 send-community extended
 auto-summary
 exit-address-family
!
address-family ipv4 vrf U
 no auto-summary
 no synchronization
 exit-address-family
!
address-family ipv4 vrf D
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip local pool U-pool 2.8.1.1 2.8.1.100
ip route vrf D 2.0.0.0 255.0.0.0 Null0
!
radius-server host 22.0.20.26 auth-port 1812 acct-port 1813
radius-server key cisco
```

## Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic MPLS VPNs                     | <a href="#">Configuring MPLS Layer 3 VPNs</a><br><a href="#">Configuring Scalable Hub-and-Spoke MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a></li> <li>• <a href="#">Preserving QoS Settings in an MPLS VPN Carrier Supporting Carrier Network</a></li> <li>• <a href="#">Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</a></li> </ul> |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> </ul>                                                                                                                                                                                                          |
| MPLS VPN route maps                 | <a href="#">Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MPLS VPN load sharing               | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN MIBs                       | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Directing MPLS VPN traffic          | <ul style="list-style-type: none"> <li>• <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a></li> <li>• <a href="#">Directing MPLS VPN Traffic Using a Source IP Address</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| VPN ID                              | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Dialer applications with MPLS VPNs  | <ul style="list-style-type: none"> <li>• <a href="#">Dialing to Destinations with the Same IP Address for MPLS VPNs</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MPLS VPNs and OSPF                  | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Configuring Scalable Hub-and-Spoke MPLS VPNs

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1**      **Feature Information for Configuring Scalable Hub-and-Spoke MPLS VPNs**

| Feature Name                      | Releases             | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN: Half Duplex VRF Support | 12.3(6)<br>12.3(11)T | <p>This feature ensures that VPN clients that connect to the same PE router at the edge of the MPLS VPN use the hub site to communicate.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Overview, page 2</a></li> <li>• <a href="#">Upstream and Downstream VRFs, page 3</a></li> <li>• <a href="#">Reverse Path Forwarding Check, page 3</a></li> <li>• <a href="#">How to Ensure that MPLS VPN Clients Use the Hub PE Router, page 4</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links

---

This module describes how to configure a sham-link that ensures traffic travels between Virtual Private Network (VPN) client sites over the Multiprotocol Label Switching (MPLS) VPN backbone. This feature is for VPNs that run Open Shortest Path First (OSPF) between the provider edge (PE) and customer edge (CE) routers. By default, OSPF uses backdoor paths between VPN sites, not the MPLS VPN backbone.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone”](#) section on page 14.

## Contents

- [Prerequisites for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone, page 2](#)
- [Restrictions for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone, page 2](#)
- [Information About Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone, page 2](#)
- [How to Ensure That MPLS VPN Clients Communicate over the MPLS VPN Backbone, page 7](#)
- [Configuration Examples for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone, page 9](#)
- [Additional References, page 12](#)
- [Feature Information for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone, page 14](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone

Before you can configure a sham-link in an MPLS VPN, you must first enable OSPF as follows:

- Create an OSPF routing process.
- Specify the range of IP addresses to be associated with the routing process.
- Assign area IDs to be associated with the range of IP addresses.

## Restrictions for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone

When OSPF is used as a protocol between PE and CE routers, the OSPF metric is preserved when routes are advertised over the VPN backbone. The metric is used on the remote PE routers to select the correct route. For this reason, you should not modify the metric value when OSPF is redistributed to Border Gateway Protocol (BGP), and when BGP is redistributed to OSPF. If you modify the metric value, routing loops may occur.

## Information About Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone

Before configuring this feature, you should understand the following concepts:

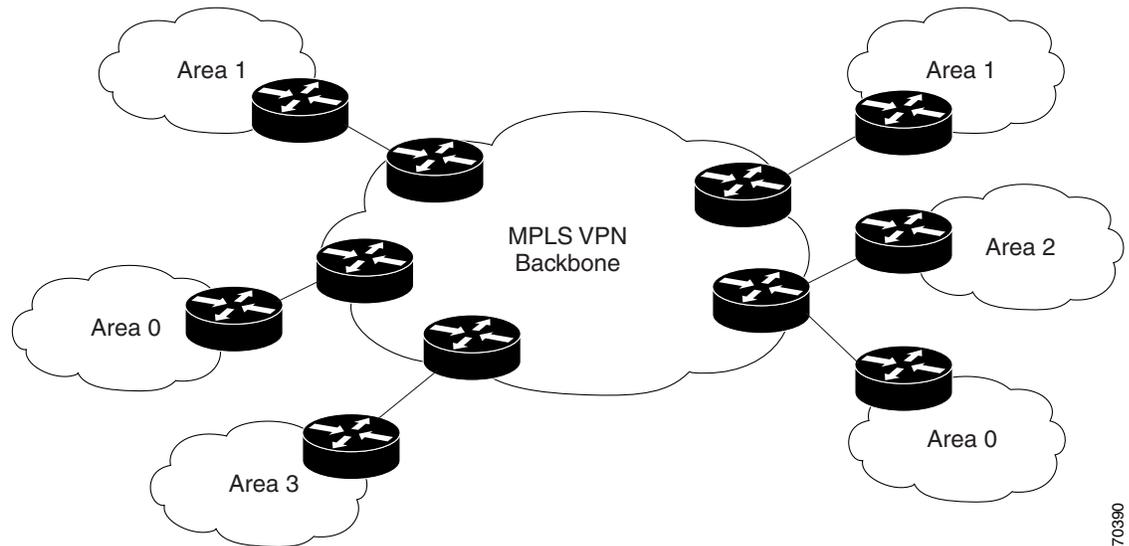
- [Introduction to MPLS VPNs Using OSPF Between PE and CE Routers, page 2](#)
- [OSPF Uses Backdoor Paths to Communicate Between VPN Sites, page 3](#)
- [Sham-Links Direct Traffic Between VPN Sites over the MPLS VPN Backbone, page 5](#)

## Introduction to MPLS VPNs Using OSPF Between PE and CE Routers

In an MPLS VPN configuration, the OSPF protocol is one way you can connect CE routers to PE routers in the VPN backbone. OSPF is often used by customers that run OSPF as their intrasite routing protocol, subscribe to a VPN service, and want to exchange routing information between their sites using OSPF (during migration or on a permanent basis) over an MPLS VPN backbone.

[Figure 1](#) shows an example of how VPN client sites (areas 0, 1, 2, and 3) that run OSPF can connect over an MPLS VPN backbone.

**Figure 1** *OSPF Connectivity Between VPN Client Sites and an MPLS VPN Backbone*



70390

When OSPF is used to connect PE and CE routers, all routing information learned from a VPN site is placed in the VPN routing and forwarding (VRF) instance associated with the incoming interface. The PE routers that attach to the VPN use the BGP to distribute VPN routes to each other. A CE router can then learn the routes to other sites in the VPN by peering with its attached PE router. The MPLS VPN backbone provides an additional level of routing hierarchy to interconnect the VPN sites running OSPF.

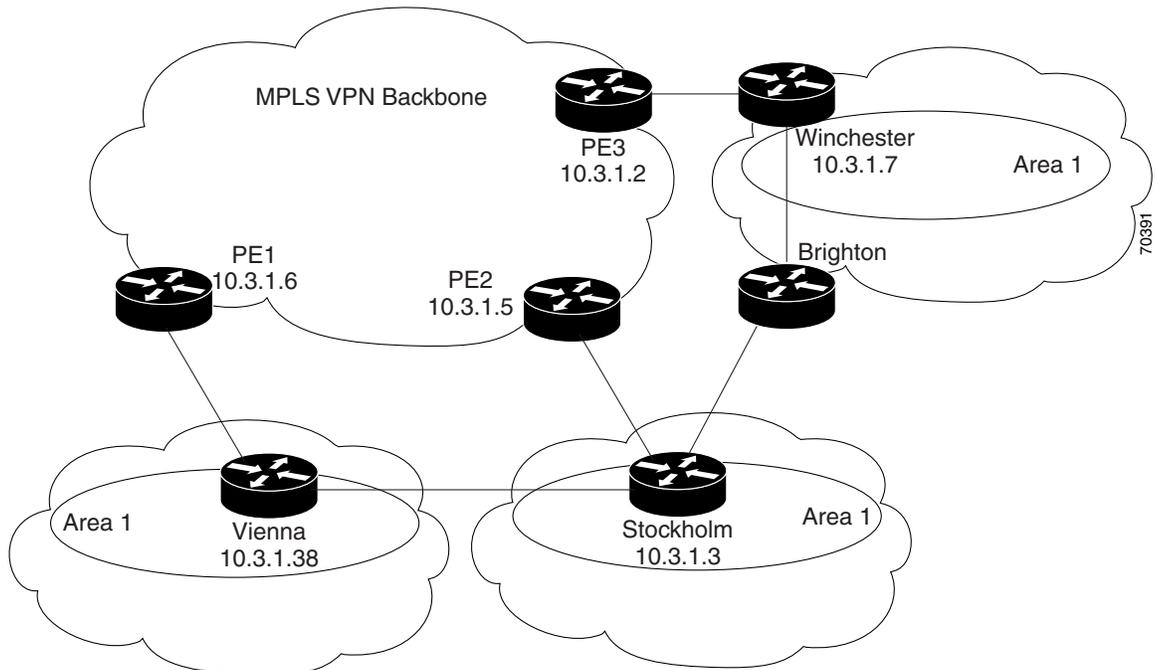
When OSPF routes are propagated over the MPLS VPN backbone, additional information about the prefix in the form of BGP extended communities (route type, domain ID extended communities) is appended to the BGP update. This community information is used by the receiving PE router to decide the type of link-state advertisement (LSA) to be generated when the BGP route is redistributed to the OSPF PECE process. In this way, internal OSPF routes that belong to the same VPN and are advertised over the VPN backbone are seen as interarea routes on the remote sites.

## OSPF Uses Backdoor Paths to Communicate Between VPN Sites

Although OSPF PECE connections assume that the only path between two client sites is across the MPLS VPN backbone, backdoor paths between VPN sites may exist. For instance, in [Figure 2](#), Vienna, Stockholm, Brighton, and Winchester can communicate through backdoor paths instead of using the MPLS VPN backbone.

If the sites belong to the same OSPF area, the backdoor path will always be selected, because OSPF prefers intra-area paths to interarea paths. (PE routers advertise OSPF routes learned over the VPN backbone as interarea paths.) For this reason, OSPF backdoor paths between VPN sites must be taken into account so that routing is performed based on policy.

**Figure 2** *Backdoor Paths Between OSPF Client Sites*



For example, [Figure 2](#) shows three client sites, each with backdoor links. Because each site runs OSPF within the same Area 1 configuration, all routing between the three sites uses the backdoor paths, rather than the MPLS VPN backbone.

The following example shows BGP routing table entries for the Winchester router (prefix 10.3.1.7/32) from the standpoint of the PE1 router in [Figure 2](#). Prefix 10.3.1.7 is the loopback interface of the Winchester CE router. As shown in bold in this example, the loopback interface is learned via BGP from PE2 and PE3. It is also generated through redistribution into BGP on PE1.

```
PE1# show ip bgp vpnv4 all 10.3.1.7

BGP routing table entry for 100:251:10.3.1.7/32, version 58
Paths: (3 available, best #2)
 Advertised to non peer-group peers:
 10.3.1.2 10.3.1.5
 Local
 10.3.1.5 (metric 30) from 10.3.1.5 (10.3.1.5)
 Origin incomplete, metric 22, localpref 100, valid, internal
 Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
 RT:1:2:0 OSPF 2
 Local
 10.2.1.38 from 0.0.0.0 (10.3.1.6)
 Origin incomplete, metric 86, localpref 100, weight 32768,
 valid, sourced, best
 Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
 RT:1:2:0 OSPF 2
 Local
 10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
 Origin incomplete, metric 11, localpref 100, valid, internal
 Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
 RT:1:2:0 OSPF 2
```

Within BGP, the locally generated route (10.2.1.38) is considered to be the best route.

However, as shown in bold in the next example, the VRF routing table shows that the selected path is learned via OSPF with a next hop of 10.2.1.38, which is the Vienna CE router.

```
PE1# show ip route vrf ospf 10.3.1.7

Routing entry for 10.3.1.7/32
 Known via "ospf 100", distance 110, metric 86, type intra area
 Redistributing via bgp 215
 Advertised by bgp 215
 Last update from 10.2.1.38 on Serial0/0/0, 00:00:17 ago
 Routing Descriptor Blocks:
 * 10.2.1.38, from 10.3.1.7, 00:00:17 ago, via Serial0/0/0
 Route metric is 86, traffic share count is 1
```

This path is selected because:

- The OSPF backdoor path is preferred over the interarea path (over the MPLS VPN backbone) generated by the PE1 router.
- OSPF has a lower administrative distance (AD) than internal BGP (BGP running between routers in the same autonomous system).

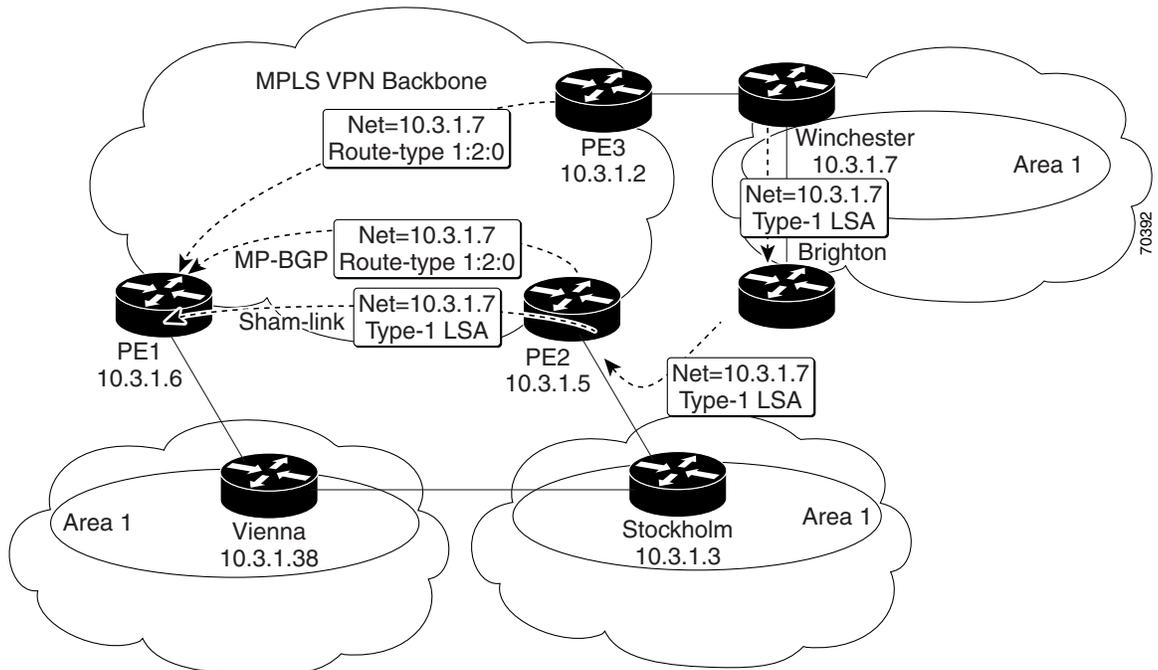
If the backdoor paths between sites are used only for backup purposes and do not participate in the VPN service, then the default route selection is acceptable. You can set up the OSPF cost configured with a sham-link to send VPN site traffic over a backdoor path.

## Sham-Links Direct Traffic Between VPN Sites over the MPLS VPN Backbone

To ensure that VPN sites that belong to the same OSPF area and share an OSPF backdoor path communicate with each other using the MPLS VPN backbone, you must create a sham-link. (If no backdoor path exists between the sites, no sham-link is required.) A sham-link is an additional OSPF intra-area (logical) link between ingress and egress VRFs on the PE routers that connect to the CE routers of the VPN sites.

[Figure 3](#) shows a sample sham-link between PE1 and PE2. You associate a cost with each sham-link to force traffic to use the sham-link rather than the backdoor path. When a sham-link is configured between PE routers, the PE routers can populate the VRF routing table with the OSPF routes learned over the sham-link.

Figure 3 Using a Sham-Link Between PE Routers to Connect OSPF Client Sites



Because the sham-link is seen as an intra-area link between PE routers, an OSPF adjacency is created and database exchange (for the particular OSPF process) occurs across the link. The PE router can then flood LSAs between sites from across the MPLS VPN backbone. As a result, the desired intra-area connectivity is created.

# How to Ensure That MPLS VPN Clients Communicate over the MPLS VPN Backbone

This section explains how to create a sham-link on an MPLS VPN PE router. Perform this task on both PE routers that share the sham-link.

## Prerequisites

Before you create a sham-link between PE routers in an MPLS VPN, you must:

- Configure a separate /32 address on the remote PE so that OSPF packets can be sent over the VPN backbone to the remote end of the sham-link. The /32 address must meet the following criteria:
  - Belong to a VRF.
  - Not be advertised by OSPF.
  - Be advertised by BGP.

You can use the /32 address for other sham-links.

- Associate the sham-link with an existing OSPF area.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **end**
7. **router ospf** *process-id* **vrf** *vrf-name*
8. **area** *area-id* **sham-link** *source-address destination-address cost number*
9. **show ip ospf sham-links**

## DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|        | Command or Action                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 1                                                        | Creates a loopback interface to be used as an endpoint of the sham-link on the PE router and enters interface configuration mode.                                                                                                                                                                                     |
| Step 4 | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding ospf                                                            | Associates the loopback interface with a VRF. Removes the IP address.                                                                                                                                                                                                                                                 |
| Step 5 | <b>ip address</b> <i>ip-address mask</i><br><br><b>Example:</b><br>Router(config-if)# ip address 10.2.1.2<br>255.255.255.255                                            | Reconfigures the IP address of the loopback interface on the PE router.                                                                                                                                                                                                                                               |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                                             | Returns to global configuration mode.                                                                                                                                                                                                                                                                                 |
| Step 7 | <b>router ospf process-id vrf vrf-name</b><br><br><b>Example:</b><br>Router(config)# router ospf 100 vrf ospf                                                           | Configures the specified OSPF process with the VRF associated with the sham-link interface on the PE router and enters interface configuration mode.                                                                                                                                                                  |
| Step 8 | <b>area area-id sham-link source-address destination-address cost number</b><br><br><b>Example:</b><br>Router(config-if)# area 1 sham-link 10.2.1.2<br>10.2.1.1 cost 40 | Configures the sham-link on the PE router interface within a specified OSPF area and with the loopback interfaces specified by the IP addresses as endpoints. <ul style="list-style-type: none"> <li><b>cost number</b> configures the OSPF cost for sending an IP packet over the PE sham-link interface.</li> </ul> |
| Step 9 | <b>show ip ospf sham-links</b>                                                                                                                                          | Verifies that the sham-link was successfully created and is operational.                                                                                                                                                                                                                                              |

### Example

The following is sample output from the **show ip ospf sham-links** command:

```
Router# show ip ospf sham-links

Sham Link OSPF_SL0 to address 10.2.1.2 is up
Area 1 source address 10.2.1.1
Run as demand circuit
DoNotAge LSA allowed.
Cost of using 40 State POINT_TO_POINT,
Timer intervals configured,
Hello 10, Dead 40, Wait 40,
Hello due in 00:00:04
Adjacency State FULL (Hello suppressed)
Index 2/2, retransmission queue length 4, number of retransmission 0
First 0x63311F3C(205)/0x63311FE4(59) Next
0x63311F3C(205)/0x63311FE4(59)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
Link State retransmission due in 360 msec
```

# Configuration Examples for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone

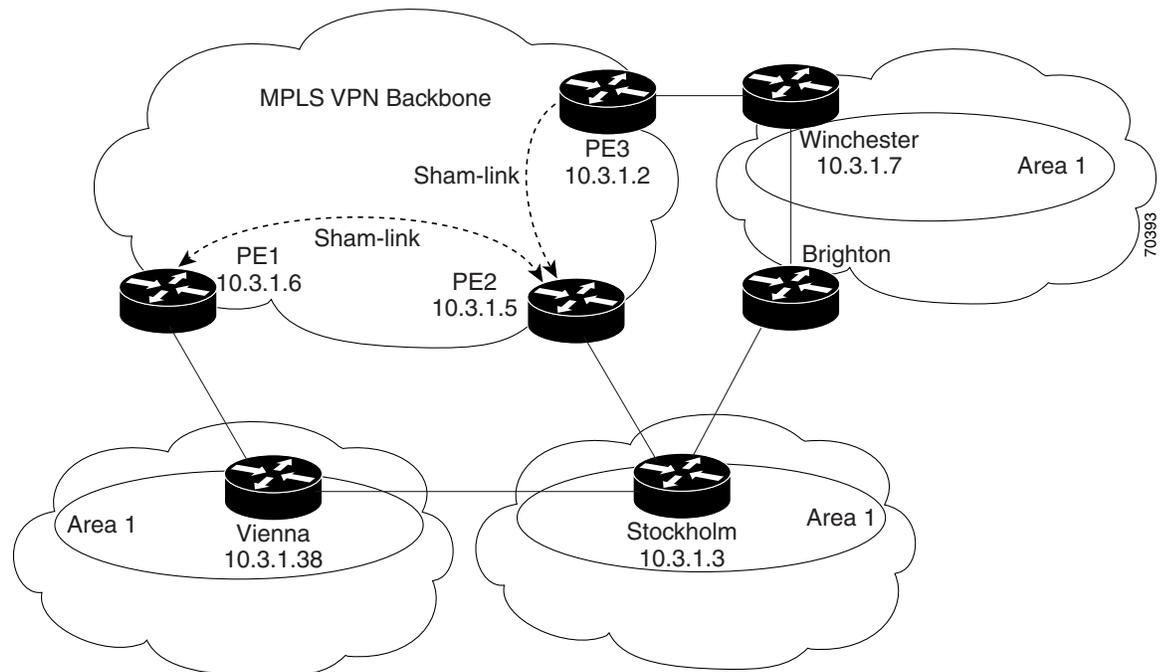
The following example shows how to configure a sham-link between two PE routers:

```
Router1(config)# interface loopback 1
Router1(config-if)# ip vrf forwarding ospf
Router1(config-if)# ip address 10.2.1.1 255.255.255.255
!
Router2(config)# interface loopback 1
Router2(config-if)# ip vrf forwarding ospf
Router2(config-if)# ip address 10.2.1.2 255.255.255.255
!
Router1(config)# router ospf 100 vrf ospf
Router1(config-if)# area 1 sham-link 10.2.1.1 10.2.1.2 cost 40
!
Router2(config)# router ospf 100 vrf ospf
Router2(config-if)# area 1 sham-link 10.2.1.2 10.2.1.1 cost 40
```

This example shows how a sham-link is used only to affect the OSPF intra-area path selection of the PE and CE routers. The PE router also uses the information received from Multiprotocol BGP (MP-BGP) to set the outgoing label stack of incoming packets, and to decide to which egress PE router to label-switch the packets.

Figure 4 shows a sample MPLS VPN topology in which a sham-link configuration is necessary. A VPN client has three sites, each with a backdoor path. Two sham-links have been configured, one between PE1 and PE2, and another between PE2 and PE3. A sham-link between PE1 and PE3 is not necessary in this configuration, because the Vienna and Winchester sites do not share a backdoor path.

**Figure 4** Sham-Link Example



The following example shows the forwarding that occurs between sites from the standpoint of how PE1 views the 10.3.1.7/32 prefix, the loopback1 interface of the Winchester CE router in [Figure 4](#).

```
PE1# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 124
Paths: (1 available, best #1)
 Local
 10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
 Origin incomplete, metric 11, localpref 100, valid, internal,
 best
 Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
 RT:1:2:0 OSPF 2
```

```
PE1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
 Known via "ospf 100", distance 110, metric 13, type intra area
 Redistributing via bgp 215
 Last update from 10.3.1.2 00:12:59 ago
 Routing Descriptor Blocks:
 10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:12:59 ago
```

The next example shows forwarding information in which the next hop for the route, 10.3.1.2, is the PE3 router rather than the PE2 router (which is the best path according to OSPF). The OSPF route is not redistributed to BGP on the PE, because the other end of the sham-link already redistributed the route to BGP and there is no need for duplication. The OSPF sham-link is used only to influence intra-area path selection. When sending traffic to a particular destination, the PE router uses the MP-BGP forwarding information.

```
PE1# show ip bgp vpnv4 all tag | begin 10.3.1.7
10.3.1.7/32 10.3.1.2 notag/38
```

```
PE1# show mpls forwarding 10.3.1.2
```

| Local label | Outgoing label or VC | Prefix or Tunnel Id | Bytes label switched | Outgoing interface | Next Hop    |
|-------------|----------------------|---------------------|----------------------|--------------------|-------------|
| 31          | 42                   | 10.3.1.2/32         | 0                    | PO3/0/0            | point2point |

```
PE1# show ip cef vrf ospf 10.3.1.7
```

```
10.3.1.7/32, version 73, epoch 0, cached adjacency to POS3/0/0
0 packets, 0 bytes
tag information set
 local tag: VPN-route-head
 fast tag rewrite with PO3/0/0, point2point, tags imposed: {42 38}
 via 10.3.1.2, 0 dependencies, recursive
 next hop 10.1.1.17, POS3/0/0 via 10.3.1.2/32
 valid cached adjacency
 tag rewrite with PO3/0/0, point2point, tags imposed: {42 38}
```

If a prefix is learned across the sham-link and the path via the sham-link is selected as the best, the PE router does not generate an MP-BGP update for the prefix. It is not possible to route traffic from one sham-link over another sham-link.

In the following example, PE2 shows how an MP-BGP update for the prefix is not generated. Although 10.3.1.7/32 has been learned via OSPF across the sham-link as shown in bold, no local generation of a route into BGP is performed. The only entry within the BGP table is the MP-BGP update received from PE3 (the egress PE router for the 10.3.1.7/32 prefix).

```
PE2# show ip route vrf ospf 10.3.1.7

Routing entry for 10.3.1.7/32
 Known via "ospf 100", distance 110, metric 12, type intra area
 Redistributing via bgp 215
 Last update from 10.3.1.2 00:00:10 ago
 Routing Descriptor Blocks:
 * 10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:00:10 ago
 Route metric is 12, traffic share count is 1

PE2# show ip bgp vpnv4 all 10.3.1.7

BGP routing table entry for 100:251:10.3.1.7/32, version 166
Paths: (1 available, best #1)
 Not advertised to any peer
 Local
 10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
 Origin incomplete, metric 11, localpref 100, valid, internal,
 best
 Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
 RT:1:2:0 OSPF 2
```

The PE router uses the information received from MP-BGP to set the ongoing label stack of incoming packets, and to decide to which egress PE router to label-switch the packets.

## Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic MPLS VPNs                     | <a href="#">Configuring MPLS Layer 3 VPNs</a><br><a href="#">Configuring Scalable Hub-and-Spoke MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a></li> <li>• <a href="#">Preserving QoS Settings in an MPLS VPN Carrier Supporting Carrier Network</a></li> <li>• <a href="#">Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</a></li> </ul> |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> </ul>                                                                                                                                                                                                          |
| MPLS VPN route maps                 | <a href="#">Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MPLS VPN load sharing               | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN MIBs                       | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Directing MPLS VPN traffic          | <ul style="list-style-type: none"> <li>• <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a></li> <li>• <a href="#">Directing MPLS VPN Traffic Using a Source IP Address</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| VPN ID                              | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Dialer applications with MPLS VPNs  | <ul style="list-style-type: none"> <li>• <a href="#">Dialing to Destinations with the Same IP Address for MPLS VPNs</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MPLS VPNs and OSPF                  | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                      |
|----------|------------------------------------------------------------|
| RFC 1164 | Application of the Border Gateway Protocol in the Internet |
| RFC 1171 | A Border Gateway Protocol 4                                |
| RFC 1700 | Assigned Numbers                                           |
| RFC 1966 | BGP Route Reflection: An Alternative to Full Mesh IBGP     |
| RFC 2283 | Multiprotocol Extensions for BGP-4                         |
| RFC 2328 | Open Shortest Path First, Version 2                        |
| RFC 2547 | BGP/MPLS VPNs                                              |
| RFC 2842 | Capabilities Advertisement with BGP-4                      |
| RFC 2858 | Multiprotocol Extensions for BGP-4                         |
| RFC 3107 | Carrying Label Information in BGP-4                        |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone

| Feature Name                                                     | Releases                            | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ensuring MPLS VPN Clients Communicate over the MPLS VPN Backbone | 12.2(8)T<br>12.0(21)ST<br>12.0(22)S | <p>This feature allows you to configure a sham-link that directs traffic between Virtual Private Network (VPN) client sites over the Multiprotocol Label Switching (MPLS) VPN backbone.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Introduction to MPLS VPNs Using OSPF Between PE and CE Routers, page 2</a></li> <li>• <a href="#">OSPF Uses Backdoor Paths to Communicate Between VPN Sites, page 3</a></li> <li>• <a href="#">Sham-Links Direct Traffic Between VPN Sites over the MPLS VPN Backbone, page 5</a></li> <li>• <a href="#">How to Ensure That MPLS VPN Clients Communicate over the MPLS VPN Backbone, page 7</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





# Assigning an ID Number to a VPN

---

You can identify virtual private networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the VPN ID feature is used for identifying a VPN.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for Assigning an ID Number to a VPN”](#) section on page 9.

## Contents

- [Information About VPN ID, page 1](#)
- [How to Configure a VPN ID, page 3](#)
- [Additional References, page 7](#)
- [Feature Information for Assigning an ID Number to a VPN, page 9](#)

## Information About VPN ID

Before configuring this feature, you should understand the following concepts:

- [Introduction to VPN ID, page 2](#)
- [Components of the VPN ID, page 2](#)
- [Management Applications That Use VPN IDs, page 2](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

## Introduction to VPN ID

You can identify VPNs by a VPN identification number, as described in RFC 2685. This implementation of the VPN ID feature is used for identifying a VPN. The VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with VPN ID numbers in the MP-BGP VPNv4 routing updates.

Multiple VPNs can be configured in a router. A VPN is private and uses a private address space that might also be used by another VPN or by the Internet. The IP address used in a VPN is only significant to the VPN in which it exists. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

**Note**

---

Configuration of a VPN ID for a VPN is optional. You can still use a VPN name to identify configured VPNs in the router. The VPN name is not affected by the VPN ID configuration. These are two independent mechanisms to identify VPNs.

---

## Components of the VPN ID

Each VPN ID defined by RFC 2685 consists of the following elements:

- An Organizational Unique Identifier (OUI), a three-octet hex number

The IEEE Registration Authority assigns OUIs to any company that manufactures components under the ISO/IEC 8802 standard. The OUI is used to generate universal LAN MAC addresses and protocol identifiers for use in local and metropolitan area network applications. For example, an OUI for Cisco Systems is 00-03-6B (hex).

- A VPN index, a four-octet hex number, which identifies the VPN within the company.

Use the following **vpn id** command and specify the VPN ID:

```
vpn id oui:vpn-index
```

A colon separates the OUI from the VPN index.

## Management Applications That Use VPN IDs

You can use several applications to manage VPNs by VPN ID. Remote access applications, such as the Remote Authentication Dial-In User Service (RADIUS) and Dynamic Host Configuration Protocol (DHCP), can use the VPN ID feature to identify a VPN. RADIUS can use the VPN ID to assign dial-in users to the proper VPN, based on each user's authentication information.

## Dynamic Host Configuration Protocol

Using DHCP network administrators can centrally manage and automate the assignment of IP addresses in an organization's network. The DHCP application uses the VPN ID as follows:

1. A VPN DHCP client requests a connection to a provider edge (PE) router from a VRF interface.
2. The PE router determines the VPN ID associated with that interface.
3. The PE router sends a request with the VPN ID and other information for assigning an IP address to the DHCP server.
4. The DHCP server uses the VPN ID and IP address information to process the request.
5. The DHCP server sends a response back to the PE router, allowing the VPN DHCP client access to the VPN.

## Remote Authentication Dial-In User Service

A RADIUS server (or daemon) provides authentication and accounting services to one or more client network access servers (NASs). RADIUS servers authenticate users and return all configuration information necessary for the client to deliver service to the users.

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server.

- The Access-Request packet contains the username, encrypted password, NAS IP address, VPN ID, and port. The format of the request also provides information on the type of session that the user wants to initiate.
- The RADIUS server returns an Access-Accept response if it finds the username and verifies the password. The response includes a list of attribute-value pairs that describe the parameters to be used for this session. If the user is not authenticated, an Access-Reject is sent by the RADIUS server and access is denied.

## How to Configure a VPN ID

This section contains the following procedures:

- [Specifying a VPN ID, page 3](#) (required)
- [Verifying the VPN ID Configuration, page 5](#) (optional)

## Specifying a VPN ID

Use this procedure to specify a VPN ID.

## Restrictions

The VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with VPN ID numbers in the MP-BGP VPNv4 routing updates.

## Prerequisites

Each VRF configured on a PE router can have a VPN ID configured. Configure all the PE routers that belong to the same VPN with the same VPN ID. Make sure the VPN ID is unique to the service provider network.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf *vrf-name***
4. **vpn id *oui:vpn-index***

## DETAILED STEPS

|        | Command                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>ip vrf <i>vrf-name</i></b><br><br><b>Example:</b><br>Router(config)# ip vrf storm                   | Creates a VRF routing table and a CEF forwarding table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>• <i>vrf-name</i>—Name assigned to a VRF.</li> </ul>                                                                                                                                                                              |
| Step 4 | <b>vpn id <i>oui:vpn-index</i></b><br><br><b>Example:</b><br>Router(config-vrf)# vpn id <b>a1:3f6c</b> | Assigns the VPN ID to the VRF. <ul style="list-style-type: none"> <li>• <i>oui</i>—An organizationally unique identifier. The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets.</li> <li>• <i>vpn-index</i>—This value identifies the VPN within the company. This VPN index is restricted to four octets.</li> </ul> |

## Example

The following example updates the VPN ID assigned to the VRF table called vpn1:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf vpn1
Router(config-vrf)# vpn id a1:3f6c
```

## Verifying the VPN ID Configuration

To verify the VPN ID configuration, perform the following steps.

### SUMMARY STEPS

1. **show ip vrf**
2. **show ip vrf id**
3. **show ip vrf detail**

### DETAILED STEPS

#### Step 1 **show ip vrf**

Use this command to display information about the VRF tables on the PE router. This example displays three VRF tables called vpn1, vpn2, and vpn5.

```
Router# show ip vrf
```

| Name | Default RD | Interfaces                 |
|------|------------|----------------------------|
| vpn1 | 100:1      | Ethernet1/1<br>Ethernet1/4 |
| vpn2 | <not set>  |                            |
| vpn5 | 500:1      | Loopback2                  |

#### Step 2 **show ip vrf id**

Use this command to ensure that the PE router contains the VPN ID you specified. The following example shows that only VRF tables vpn1 and vpn2 have VPN IDs assigned. The VRF table called vpn5 is not displayed, because it does not have a VPN ID.

```
Router# show ip vrf id
```

| VPN Id  | Name | RD        |
|---------|------|-----------|
| 2:3     | vpn2 | <not set> |
| A1:3F6C | vpn1 | 100:1     |

**Step 3 show ip vrf detail**

Use this command to see all the VRFs on a PE router. This command displays all the VPN IDs that are configured on the router, their associated VRF names, and VRF route distinguishers (RDs). If a VRF table in the PE router has not been assigned a VPN ID, that VRF entry is not included in the output.

```
Router# show ip vrf detail

VRF vpn1; default RD 100:1; default VPNID A1:3F6C
 Interfaces:
 Ethernet1/1 Ethernet1/4
 Connected addresses are not in global routing table
 Export VPN route-target communities
 RT:100:1
 Import VPN route-target communities
 RT:100:1 RT:500:1
 No import route-map
 No export route-map
VRF vpn2; default RD <not set>; default VPNID 2:3
 No interfaces
 Connected addresses are not in global routing table
 No Export VPN route-target communities
 No Import VPN route-target communities
 No import route-map
 No export route-map
VRF vpn5; default RD 500:1; default VPNID <not set>
 Interfaces:
```

# Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic MPLS VPNs                     | <i>Configuring MPLS Layer 3 VPNs</i><br><i>Configuring Scalable Hub-and-Spoke MPLS VPNs</i>                                                                                                                                                                                                                                                                               |
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li><i>MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</i></li> <li><i>MPLS VPN Carrier Supporting Carrier with BGP</i></li> <li>Preserving QoS Settings in an MPLS VPN Carrier Supporting Carrier Network</li> <li><i>Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</i></li> </ul> |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li><i>MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</i></li> <li><i>MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</i></li> </ul>                                                                                                                                                                   |
| MPLS VPN route maps                 | <i>Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN</i>                                                                                                                                                                                                                                                                   |
| MPLS VPN load sharing               | <i>Load Sharing MPLS VPN Traffic</i>                                                                                                                                                                                                                                                                                                                                      |
| MPLS VPN MIBs                       | <i>Monitoring MPLS VPNs with MIBs</i>                                                                                                                                                                                                                                                                                                                                     |
| Directing MPLS VPN traffic          | <ul style="list-style-type: none"> <li><i>Directing MPLS VPN Traffic Using Policy-Based Routing</i></li> <li><i>Directing MPLS VPN Traffic Using a Source IP Address</i></li> </ul>                                                                                                                                                                                       |
| Dialer applications with MPLS VPNs  | <i>Dialing to Destinations with the Same IP Address for MPLS VPNs</i>                                                                                                                                                                                                                                                                                                     |
| MPLS VPNs and OSPF                  | <i>Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</i>                                                                                                                                                                                                                                                 |
| MPLS VPN High Availability          | <i>Preserving MPLS VPN Label Information During Failover</i>                                                                                                                                                                                                                                                                                                              |

## Standards

| Standard          | Title                                                                |
|-------------------|----------------------------------------------------------------------|
| IEEE Std 802-1990 | IEEE Local and Metropolitan Area Networks: Overview and Architecture |

## MIBs

| MIB  | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                               |
|----------|-------------------------------------|
| RFC 2685 | Virtual Private Networks Identifier |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for Assigning an ID Number to a VPN

[Table 1](#) lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Assigning an ID Number to a VPN

| Feature Name | Releases                                        | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VPN ID       | 12.0(17)ST<br>12.2(4)B<br>12.2(8)T<br>12.2(14)S | This feature lets you identify VPNs by a VPN identification number, as described in RFC 2685.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Components of the VPN ID, page 2</a></li> <li>• <a href="#">Management Applications That Use VPN IDs, page 2</a></li> <li>• <a href="#">How to Configure a VPN ID, page 3</a></li> </ul> |
| MPLS VPN ID  | Cisco IOS                                       | For information about feature support in Cisco IOS software, use Cisco Feature Navigator.                                                                                                                                                                                                                                                                                                                         |
| MPLS VPN ID  | Cisco IOS XE Release 2.1                        | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                     |

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# Directing MPLS VPN Traffic Using Policy-Based Routing

---

This module explains how to configure policy-based routing (PBR) to classify and forward Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) traffic based on multiple VPN routing and forwarding (VRF) selection match criteria.

## Module History

This module was first published on May 2, 2005, and last updated on September 10, 2007.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for Directing MPLS VPN Traffic Using Policy-Based Routing”](#) section on page 17.

## Contents

- [Prerequisites for Directing MPLS VPN Traffic Using Policy-Based Routing, page 2](#)
- [Restrictions for Directing MPLS VPN Traffic Using Policy-Based Routing, page 2](#)
- [Information About Directing MPLS VPN Traffic Using Policy-Based Routing, page 2](#)
- [How to Configure Policy-Based Routing To Direct MPLS VPN Traffic, page 3](#)
- [Configuration Examples for Directing MPLS VPN Traffic Using Policy-Based Routing, page 12](#)
- [Additional References, page 15](#)
- [Feature Information for Directing MPLS VPN Traffic Using Policy-Based Routing, page 17](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Directing MPLS VPN Traffic Using Policy-Based Routing

- Multiprotocol BGP (MP-BGP), Multiprotocol Label Switching (MPLS), Cisco Express Forwarding (CEF), and MPLS VPNs must be enabled in your network.
- The router must be running Cisco IOS software that supports policy-based routing (PBR).
- A VRF must be defined prior to the configuration of this feature. An error message is displayed in the console if no VRF exists.

## Restrictions for Directing MPLS VPN Traffic Using Policy-Based Routing

- VRF Select is supported only in Service Provider (-p-) images.
- This feature can coexist with features that use VRF selection based on the source IP address, but these features cannot be configured together on the same interface. This is designed behavior to prevent VRF table selection conflicts that could occur if these features were misconfigured together. The console returns an error message if you attempt to configure the **ip vrf select source** and the **ip vrf policy-map** commands on the same interface.
- Protocol Independent Multicast (PIM) and multicast packets do not support PBR and cannot be configured for a source IP address that is match criteria for this feature.
- The **set vrf** command cannot be configured with the following commands in the same route map sequence:
  - **set ip default interface**
  - **set interface**
  - **set ip default next-hop**
  - **set ip next-hop**A packet cannot be set to an interface or to a next hop when the **set vrf** command is specified. This is designed behavior. An error message is displayed if you attempt to configure the **set vrf** command with any of the above four set clauses.
- The *VRF Selection using Policy Based Routing* feature cannot be configured with IP prefix lists.

## Information About Directing MPLS VPN Traffic Using Policy-Based Routing

Before configuring this feature, you should understand the following concepts:

- [Directing MPLS VPN Traffic Using Policy-Based Routing Overview, page 3](#)
- [VRF Selection Introduces a New PBR Set Clause, page 3](#)

## Directing MPLS VPN Traffic Using Policy-Based Routing Overview

This feature allows you to route VPN traffic based on the following match criteria:

- IP Access Lists — IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access list configuration options in Cisco IOS software can be used to define match criteria.
- Packet Lengths— Length of a packet in bytes. The packet length filter is defined in a route map with the **match length** route map configuration command.

Policy routing is defined in the route map. The route map is applied to the incoming interface with the **ip policy route-map** interface configuration command. IP access list match criteria is applied to the route map with the **match ip address** route map configuration command. Packet length match criteria is applied to the route map with the **match length** route map configuration command. The set action is defined with the **set vrf** route map configuration command. The match criteria is evaluated, and the appropriate VRF is selected by the set clause. This combination allows you to define match criteria for incoming VPN traffic and policy route VPN packets out to the appropriate VRF.

## VRF Selection Introduces a New PBR Set Clause

When configuring PBR, the following four set clauses can be used to change normal routing and forwarding behavior:

- set ip default interface
- **set ip interface**
- set ip default next-hop
- set ip next-hop

Configuring any of the above set clauses will overwrite normal routing forwarding behavior of a packet.

This feature introduces the fifth set clause that can be used to change normal routing and forwarding behavior. You can use the **set vrf** command to select the appropriate VRF after the successful match occurs in the route map. However, the **set vrf** command cannot be configured with the above four PBR set clauses. This is designed behavior, because a packet cannot be set to an interface or a specific next hop when it is configured within a VRF. An error message will be displayed in the console if you attempt to configure the **set vrf** command with any of the above four PBR set clauses within the same route map.

## How to Configure Policy-Based Routing To Direct MPLS VPN Traffic

This section contains the following procedures:

- [Defining the Match Criteria, page 4](#) (required)
- [Configuring the Route Map and Specifying VRFs, page 7](#) (required)
- [Applying a Route Map to an Interface, page 8](#) (required)
- [Configuring IP VRF Receive on the Interface, page 10](#) (required)
- [Verifying the Configuration, page 11](#) (optional)

## Defining the Match Criteria

The match criteria is defined in an access list. Standard and extended access lists are supported. The following sections show how to configure each type of access list:

- [Defining Match Criteria with a Standard Access List, page 4](#)
- [Defining Match Criteria with an Extended Access List, page 6](#)

Match criteria can also be defined based on the packet length by configuring the **match length** route-map configuration command. You use a route map to configure VRF selection based on packet length. See the “[Configuring the Route Map and Specifying VRFs](#)” section on [page 7](#) for more information.

## Prerequisites

The following tasks assume that the VRF and associated IP address are already defined.

### Defining Match Criteria with a Standard Access List

This task uses a standard access list to define match criteria.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `access-list access-list-number {deny | permit} source [source-wildcard] [log]`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                    | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                                               | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>}<br/><i>source</i> [<i>source-wildcard</i>] [<b>log</b>]</p> <p><b>Example:</b><br/>Router(config)# access-list 40 192.168.1.0<br/>0.0.0.255 permit</p> | <p>Creates an access list and defines the match criteria for the route map.</p> <ul style="list-style-type: none"> <li>Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access list configuration options in Cisco IOS software can be used to define match criteria.</li> <li>The example creates a standard access list numbered 40. This filter will permit traffic from any host with an IP address in the 192.168.1.0/24 subnet.</li> </ul> |

## Defining Match Criteria with an Extended Access List

This task uses an extended access list to define match criteria.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {standard | extended} [*access-list-name* | *access-list-number*]
4. [sequence-number] permit | deny protocol source source-wildcard destination destination-wildcard [option option-value] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]
5. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                                                                                                  | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>ip access-list</b> {standard extended}<br>[ <i>access-list-name</i>   <i>access-list-number</i> ]<br><br><b>Example:</b><br>Router(config)# ip access-list extended<br>NAMEDACL                                                                                                                                                                                                                              | Specifies the IP access list type, and enters the corresponding access list configuration mode. <ul style="list-style-type: none"> <li>• A standard, extended, or named access list can be used.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| Step 4 | [ <i>sequence-number</i> ] <b>permit</b>   <b>deny protocol source</b><br><b>source-wildcard destination</b><br><b>destination-wildcard</b> [ <b>option</b><br><i>option-value</i> ][ <b>precedence precedence</b> ] [ <b>tos tos</b> ]<br>[ <b>log</b> ] [ <b>time-range time-range-name</b> ] [ <b>fragments</b> ]<br><br><b>Example:</b><br>Router(config-ext-nacl)# permit ip any any<br>option any-options | Defines the criteria for which the access list will permit or deny packets. <ul style="list-style-type: none"> <li>• Match criteria can be defined based on IP addresses, IP address ranges, and other IP packet access list filtering options. Named, numbered, standard, and extended access lists are supported. All IP access list configuration options in Cisco IOS software can be used to define match criteria.</li> <li>• The example creates a named access list that permits any configured IP option.</li> </ul> |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-ext-nacl)# exit                                                                                                                                                                                                                                                                                                                                             | Exits named access list configuration mode, and enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Configuring the Route Map and Specifying VRFs

You define a route map then assign an access list to it. Then you specify a VRF for the traffic that matches the criteria in the route map. Use the **set vrf** command to specify the VRF through which the outbound VPN packets are routed.

### Prerequisites

Define the VRF before configuring the route map; otherwise the console displays an error.

### Restrictions

- If an interface is associated with a VRF by configuring the **ip vrf forwarding** interface configuration command, you cannot also configure the same interface to use PBR with the **set vrf** route map configuration command.
- The **set vrf** command cannot be configured with the following commands in the same route map sequence:
  - **set ip default interface**
  - **set interface**
  - **set ip default next-hop**
  - **set ip next-hop**

A packet cannot be set to an interface or to a next hop when the **set vrf** command is specified. This is designed behavior. An error message is displayed if you attempt to configure the **set vrf** command with any of the above four set clauses.

### SUMMARY STEPS

1. **enable**
  2. **configure terminal**
  3. **route-map map-tag [permit | deny] [sequence-number]**
  4. **match ip address** { *acl-number [acl-number ...] acl-name ...* | *acl-name [acl-name ...] acl-number ...* }
- or
5. **set vrf** *vrf-name*
  6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                                                                     | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                                                                                                                                                                                                | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <p><b>route-map</b> <i>map-tag</i> [<b>permit</b>   <b>deny</b>]<br/>[<i>sequence-number</i>]</p> <p><b>Example:</b><br/>Router(config)# route-map RED permit 10</p>                                                                                                                                                                                                                  | <p>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. Enters route map configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | <p><b>match ip address</b> {<i>acl-number</i> [<i>acl-number</i> ...   <i>acl-name</i> ...]   <i>acl-name</i> [<i>acl-name</i> ...   <i>acl-number</i> ...] }</p> <p><b>Example:</b><br/>Router(config-route-map)# match ip address 1<br/>or<br/>match length <i>minimum-length</i> <i>maximum-length</i></p> <p><b>Example:</b><br/>Router(config-route-map)# match length 3 200</p> | <p>Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on matched packets.</p> <ul style="list-style-type: none"> <li>IP access lists are supported.</li> <li>The example configures the route map to use standard access list 1 to define match criteria.</li> </ul> <p>or</p> <p>Specifies the Layer 3 packet length in the IP header as a match criteria in a class map.</p> <ul style="list-style-type: none"> <li>The example configures the route map to match packets that are between 3 and 200 bytes in size.</li> </ul> |
| Step 5 | <p><b>set vrf</b> <i>vrf-name</i></p> <p><b>Example:</b><br/>Router(config-route-map)# set vrf RED</p>                                                                                                                                                                                                                                                                                | <p>Defines which VRF to send VPN packets that are successfully matched.</p> <ul style="list-style-type: none"> <li>The example policy routes matched packets out to the VRF named RED.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 6 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config-route-map)# exit</p>                                                                                                                                                                                                                                                                                                          | <p>Exits route-map configuration mode and enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Applying a Route Map to an Interface

You apply a route map to the incoming interface with the **ip policy route-map** global configuration command.

## Restrictions

- This feature can coexist with the “VRF Select” feature (**ip vrf select source** command), which uses the source IP address to select VRFs on the same router. However, the two features cannot be configured together on the same interface. This is designed behavior to prevent VRF table selection conflicts that could occur if these features were misconfigured together. The console displays an error message if you attempt to configure the **ip vrf select source** and the **ip vrf policy-map** commands on the same interface.
- PBR can be configured on an interface where a VRF is defined. However, the console displays the following warning messages if you attempt to configure both PBR and a VRF on the same interface:

```
%% Policy Based Routing is NOT supported for VRF" interfaces
%% IP-Policy can be used ONLY for marking "(set/clear DF bit) on
```

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** type number [name-tag]
4. **ip policy route-map** map-tag
5. **ip vrf receive** vrf-name
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                                            | Purpose                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                       | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                               | Enters global configuration mode.                                       |
| Step 3 | <b>interface</b> type number [name-tag]<br><br><b>Example:</b><br>Router(config)# interface FastEthernet 0/1 | Configures an interface and enters interface configuration mode.        |
| Step 4 | <b>ip policy route-map</b> [map-tag]<br><br><b>Example:</b><br>Router(config-if)# ip policy route-map RED    | Identifies a route map to use for policy routing on an interface.       |

|        | Command or Action                                                                                     | Purpose                                                                                                                                                                                                                                                                |
|--------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>ip vrf receive vrf-name</pre> <p><b>Example:</b><br/>Router(config-if)# ip vrf receive VRF_1</p> | <p>Adds the IP addresses that are associated with an interface into the VRF table.</p> <ul style="list-style-type: none"> <li>This command can be configured so that the receiving packets can be received by the router after being set to a specific VRF.</li> </ul> |
| Step 6 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-if)# end</p>                                      | <p>Exits interface configuration mode and enters global configuration mode.</p>                                                                                                                                                                                        |

## Configuring IP VRF Receive on the Interface

You must add the source IP address to the VRF selection table. VRF Selection is a one-way (unidirectional) feature. It is applied to the incoming interface. If a match and set operation occurs in the route map but there is no receive entry in the local VRF table, the packet will be dropped if the packet destination is local.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `interface type number [name-tag]`
4. `ip policy route-map map-tag`
5. `ip vrf receive vrf-name`
6. **end**

|        | Command                                                                                                           | Purpose                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                                                    | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <pre>configure terminal</pre> <p><b>Example:</b><br/>Router# configure terminal</p>                               | <p>Enters global configuration mode.</p>                                                                                |
| Step 3 | <pre>interface type number [name-tag]</pre> <p><b>Example:</b><br/>Router(config)# interface FastEthernet 0/1</p> | <p>Configures an interface and enters interface configuration mode.</p>                                                 |

|        | Command                                                                                                         | Purpose                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <code>ip policy route-map [map-tag]</code><br><br><b>Example:</b><br>Router(config-if)# ip policy route-map RED | Identifies a route map to use for policy routing on an interface.                                                                                                                                                   |
| Step 5 | <code>ip vrf receive vrf-name</code><br><br><b>Example:</b><br>Router(config-if)# ip vrf receive VRF_1          | Adds the IP addresses that are associated with an interface into the VRF table. <ul style="list-style-type: none"> <li>This command must be configured for each VRF that will be used for VRF selection.</li> </ul> |
| Step 6 | <code>end</code><br><br><b>Example:</b><br>Router(config-if)# end                                               | Exits interface configuration mode and enters privileged EXEC mode.                                                                                                                                                 |

## Verifying the Configuration

To verify that the configuration is correct, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `show ip access-list [access-list-number | access-list-name]`
3. `show route-map [map-name]`
4. `show ip policy`

### DETAILED STEPS

|        | Command or Action                                                                                                              | Purpose                                                                                                                                                                                                                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                  |
| Step 2 | <code>show ip access-list [access-list-number   access-list-name]</code><br><br><b>Example:</b><br>Router# show ip access-list | Displays the contents of all current IP access lists. <ul style="list-style-type: none"> <li>This command is used to verify the match criteria that is defined in the access list. Both named and numbered access lists are supported.</li> </ul> |

|        | Command or Action                                                                      | Purpose                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>show route-map [map-name]</pre> <p><b>Example:</b><br/>Router# show route-map</p> | Displays all route maps configured or only the one specified. <ul style="list-style-type: none"> <li>This command is used to verify match and set clauses within the route map.</li> </ul> |
| Step 4 | <pre>show ip policy</pre> <p><b>Example:</b><br/>Router# show ip policy</p>            | Displays the route map used for policy routing. <ul style="list-style-type: none"> <li>This command can be used to display the route map and the associated interface.</li> </ul>          |

## Configuration Examples for Directing MPLS VPN Traffic Using Policy-Based Routing

This section provides the following configuration examples:

- [Configuring Policy-Based Routing with a Standard Access List: Example, page 13](#)
- [Verifying Policy-Based Routing: Example, page 13](#)

## Configuring Policy-Based Routing with a Standard Access List: Example

In the following example, three standard access lists are created to define match criteria for three different subnets. A route map called PBR-VRF-Selection is assigned to interface Ethernet 0/1. If interface Ethernet 0/1 receives a packet whose source IP address is part of the 10.1.0.0/24 subnet, that packet is sent to VRF\_1.

```
access-list 40 permit 10.1.0.0 0.0.255.255
access-list 50 permit 10.2.0.0 0.0.255.255
access-list 60 permit 10.3.0.0 0.0.255.255

route-map PBR-VRF-Selection permit 10
 match ip address 40
 set vrf VRF_1
!
route-map PBR-VRF-Selection permit 20
 match ip address 50
 set vrf VRF_2
!
route-map PBR-VRF-Selection permit 30
 match ip address 60
 set vrf VRF_3
!
interface Ethernet0/1
 ip address 192.168.1.6 255.255.255.252
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF_1
 ip vrf receive VRF_2
 ip vrf receive VRF_3
```

## Verifying Policy-Based Routing: Example

The following verification examples show defined match criteria and route-map policy configuration.

### Verifying Match Criteria

To verify the configuration of match criteria for PBR VRF selection, use the **show ip access-lists** command. The following **show ip access-lists** command output displays three subnet ranges defined as match criteria in three standard access-lists:

```
Router# show ip access-lists

Standard IP access list 40
 10 permit 10.1.0.0, wildcard bits 0.0.255.255
Standard IP access list 50
 10 permit 10.2.0.0, wildcard bits 0.0.255.255
Standard IP access list 60
 10 permit 10.3.0.0, wildcard bits 0.0.255.255
```

### Verifying Route-Map Configuration

To verify route-map configuration, use the **show route-map** command. The output displays the match criteria and set action for each route-map sequence. The output also displays the number of packets and bytes that have been policy routed per each route-map sequence.

```
Router# show route-map

route-map PBR-VRF-Selection, permit, sequence 10
 Match clauses:
 ip address (access-lists): 40
```

```
Set clauses:
 vrf VRF_1
 Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 20
Match clauses:
 ip address (access-lists): 50
Set clauses:
 vrf VRF_2
 Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 30
Match clauses:
 ip address (access-lists): 60
Set clauses:
 vrf VRF_3
 Policy routing matches: 0 packets, 0 bytes
```

### Verifying PBR VRF Selection Policy

The following **show ip policy** command output displays the interface and associated route map that is configured for policy routing.

```
Router# show ip policy

Interface Route map
Ethernet0/1 PBR-VRF-Selection
```

## Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic MPLS VPNs                     | <a href="#">Configuring MPLS Layer 3 VPNs</a><br><a href="#">Configuring Scalable Hub-and-Spoke MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a></li> <li>• <a href="#">Preserving QoS Settings in an MPLS VPN Carrier Supporting Carrier Network</a></li> <li>• <a href="#">Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</a></li> </ul> |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> </ul>                                                                                                                                                                                                          |
| MPLS VPN route maps                 | <a href="#">Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MPLS VPN load sharing               | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN MIBs                       | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Directing MPLS VPN traffic          | <ul style="list-style-type: none"> <li>• <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a></li> <li>• <a href="#">Directing MPLS VPN Traffic Using a Source IP Address</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| VPN ID                              | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Dialer applications with MPLS VPNs  | <ul style="list-style-type: none"> <li>• <a href="#">Dialing to Destinations with the Same IP Address for MPLS VPNs</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MPLS VPNs and OSPF                  | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Directing MPLS VPN Traffic Using Policy-Based Routing

[Table 1](#) lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Directing MPLS VPN Traffic Using Policy-Based Routing

| Feature Name                                      | Releases              | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—VRF Selection using Policy-Based Routing | 12.3(7)T<br>12.2(25)S | <p>This feature allows you to classify and forward VPN traffic based on match criteria, such as IP access lists and packet length.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing Overview, page 3</a></li> <li>• <a href="#">VRF Selection Introduces a New PBR Set Clause, page 3</a></li> <li>• <a href="#">Defining the Match Criteria, page 4</a></li> <li>• <a href="#">How to Configure Policy-Based Routing To Direct MPLS VPN Traffic, page 3</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.



# Directing MPLS VPN Traffic Using a Source IP Address

---

This module explains how to set up an interface on a provider edge (PE) router to route packets to different Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) based on the source IP address of the packet.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all features.* To find information about feature support and configuration, use the [“Feature Information for Directing MPLS VPN Traffic Using a Source IP Address”](#) section on page 16.

## Contents

- [Prerequisites for Directing MPLS VPN Traffic Using a Source IP Address, page 2](#)
- [Restrictions for Directing MPLS VPN Traffic Using a Source IP Address, page 2](#)
- [Information About Directing MPLS VPN Traffic Using a Source IP Address, page 4](#)
- [How to Enable MPLS VPN Traffic To Be Routed Using a Source IP Address, page 9](#)
- [Configuration Examples for Directing MPLS VPN Traffic Using a Source IP Address, page 13](#)
- [Additional References, page 14](#)
- [Feature Information for Directing MPLS VPN Traffic Using a Source IP Address, page 16](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Directing MPLS VPN Traffic Using a Source IP Address

- MPLS VPNs must be enabled in the provider network.
- Cisco Express Forwarding (CEF) must be enabled on any interfaces that have this feature enabled.
- The Cisco IOS software must support MPLS VPNs, and the provider network must have MPLS Label Distribution Protocol (LDP) installed and running.
- This feature is supported on the Cisco 7200 series, 7500 series, and 12000 series router platforms.

## Restrictions for Directing MPLS VPN Traffic Using a Source IP Address

VRF Select is supported only in Service Provider (-p-) images.

### Unidirectional Traffic

This is a unidirectional feature and can only be used from a customer (IP-based) network into a provider (MPLS-based) network. This feature cannot be used from a provider network to a customer network.

### Subnet Masks

Subnet masks should be kept as short as possible for Engine 2 line cards. Performance can degrade with longer subnet masks (/24 or /32, for example).

### traceroute Command

An IP **traceroute** command from a customer edge (CE) router that has this feature enabled to a typical MPLS VPN VRF CE router works as expected. However, an IP **traceroute** command from a typical MPLS VPN VRF CE router to a CE router that has this feature enabled may fail to show all the relevant hop information across the core.

### Supported Static Route Configurations

When configuring static routes in an MPLS or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.xT, 12.xM, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later. Use the following guidelines when configuring static routes.

### Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in MPLS environment:

```
ip route destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

**Unsupported Static Routes in an MPLS Environment that Uses the TFIB**

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

```
ip route destination-prefix mask next-hop1
```

```
ip route destination-prefix mask next-hop2
```

Use the *interface* and *next-hop* arguments when specifying static routes.

**Supported Static Routes in an MPLS VPN Environment**

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop and interface are in the same VRF:

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface1 next-hop1*
- **ip route vrf** *vrf-name destination-prefix mask interface2 next-hop2*

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet Gateway.

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address global*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*  
(This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 next-hop1
```

```
ip route destination-prefix mask interface2 next-hop2
```

**Unsupported Static Routes in an MPLS VPN Environment that Uses the TFIB**

The following **ip route** command is not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

```
ip route vrf destination-prefix mask next-hop-address global
```

The following **ip route** commands are not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

```
ip route vrf destination-prefix mask next-hop1 global
```

```
ip route vrf destination-prefix mask next-hop2 global
```

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

```
ip route vrf vrf-name destination-prefix mask next-hop1
ip route vrf vrf-name destination-prefix mask next-hop2
```

### Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table on the CE side. For example, the following command is supported when the destination-prefix is the CE router's loopback address, as in EBGp multihop cases.

```
ip route vrf vrf-name destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static non-recursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 nexthop1
ip route destination-prefix mask interface2 nexthop2
```

## Information About Directing MPLS VPN Traffic Using a Source IP Address

Before configuring this feature, you should understand the following concepts:

- [Introduction to Directing MPLS VPN Traffic Using a Source IP Address, page 4](#)
- [How MPLS VPN Traffic Is Routed Using the Source IP Address, page 4](#)
- [Example of MPLS VPN Traffic Being Routed Based on the Source IP Address, page 5](#)
- [Advantages of Using the Source IP Address over Per-Interface IP VPN Configuration, page 8](#)
- [Benefits of Directing MPLS VPN Traffic Using a Source IP Address, page 9](#)

### Introduction to Directing MPLS VPN Traffic Using a Source IP Address

This feature allows packets arriving on an interface to be switched into the appropriate VRF table based upon the source IP address of the packets. Once the packets have been “selected” into the correct VRF routing table, they are processed normally based upon the destination address and forwarded through the rest of the MPLS VPN.

In most cases, this is a “one way” feature; it works on packets coming from the end users to the PE router.

### How MPLS VPN Traffic Is Routed Using the Source IP Address

This feature uses the following process to route packets from the customer networks to the PE router and into the provider network.

A two-table lookup mechanism is used at the ingress interface of the PE router to determine the routing and forwarding of packets coming from the customer networks, which use IP protocols, to the MPLS VPN networks, which use MPLS protocols.

- The first table, the VRF Selection table, is used to compare the source IP address of the packet with a list of IP addresses in the table. Each IP address in the table is associated with an MPLS VPN. If a match is found between the source IP address of the packet and an IP address in the VRF Selection table, the packet is routed to the second table (the VRF table) or the routing table for the appropriate VPN.

If no match is found in the table for the source IP address of the packet, the packet will either be routed via the global routing table used by the PE router (this is the default behavior), or will be dropped. See the [“Configuring a VRF to Eliminate Unnecessary Packet Forwarding: Example” section on page 14](#) for more information.

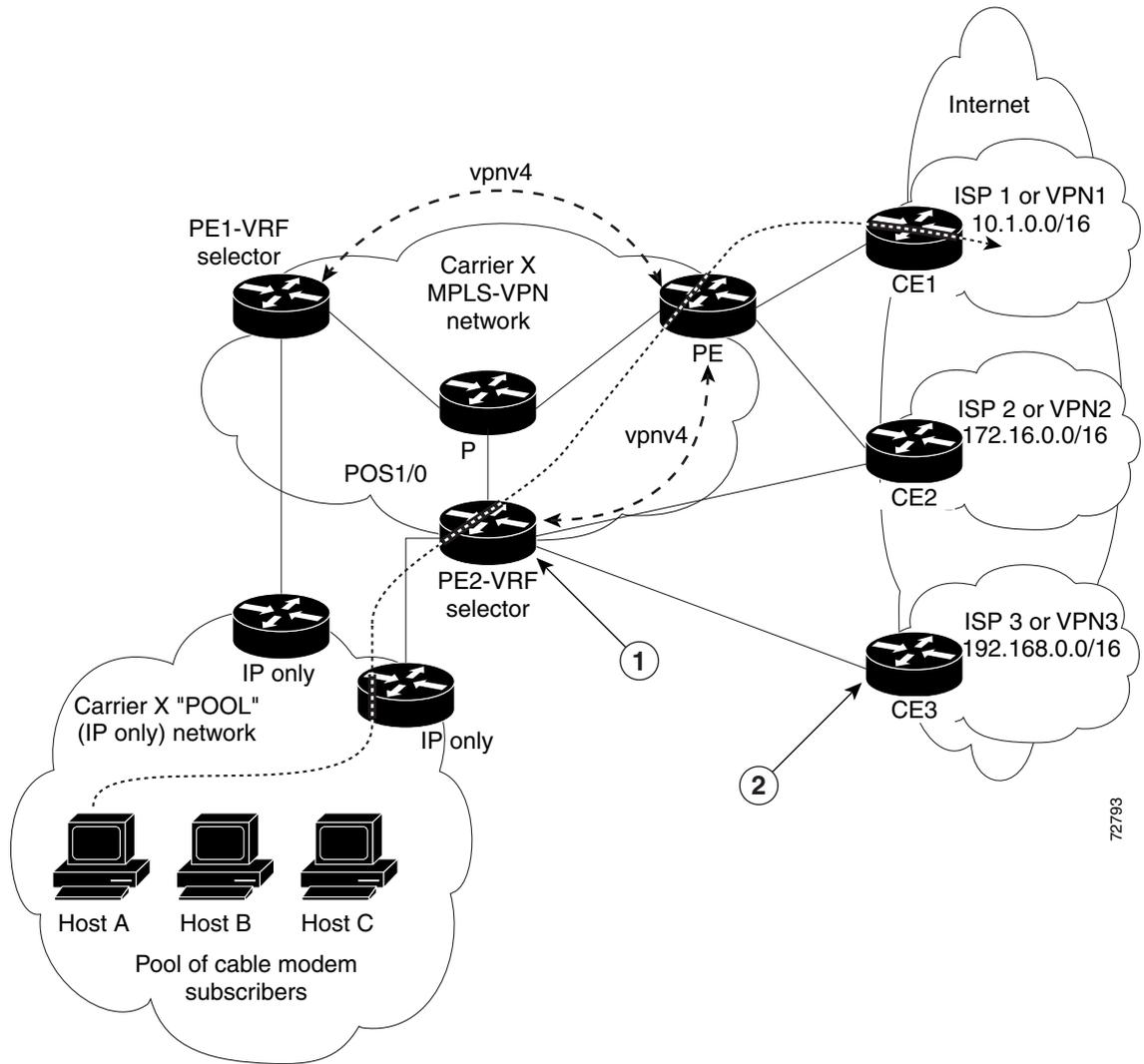
- The second table, the VRF table (also known as the VPN routing and forwarding table), contains the virtual routing and forwarding information for the specified VPN and is used to forward the selected VPN traffic to the correct MPLS label switched path (LSP) based upon the destination IP address of the packet.

The VRF Selection process removes the association between the VRF and the interface and allows more than one MPLS VPN VRF to be associated with the interface.

## Example of MPLS VPN Traffic Being Routed Based on the Source IP Address

An example of this feature is a network carrier that allows subscribers to the carrier to choose from multiple Internet service providers (ISPs) for Internet access. [Figure 1](#) provides an example of this feature with an IP-based Host network, an MPLS VPN network, and three ISPs connected to the MPLS VPN network.

Figure 1 Implementation Example



72793

In [Figure 1](#), Carrier X represents the network carrier; Host A, Host B and Host C represent the carrier subscribers; and ISP 1, ISP 2 and ISP 3 represent the ISPs.

- PE2 acts as both a VRF selector and a typical MPLS VPN PE router to CE2 and CE3.
- ISPs 1 through 3 provide a list of IP addresses to Carrier X so that each host in the “POOL” network can be properly addressed. This host addressing would most likely be done by using the DHCP or DNS services of Carrier X.

A dashed line represents the path of a packet traveling from Host A to ISP 1. Host A chooses ISP 1 to use as its ISP. Carrier X provides an IP address to Host A that falls within the range of the ISP 1 registered network addresses (1.1.0.0/16). Based upon this IP address allocation, the VRF Selection criteria is set.

By using default routes, hosts on the POOL network (such as Host A), forward traffic from the Carrier X IP-based (POOL) network to the Carrier X MPLS-based VPN network. PE2 has been configured with this feature. Therefore, the MPLS VPN network forwards the traffic from Host A to ISP 1.

This is a one-way (unidirectional) feature in most implementations; it only works on packets coming from the customer networks to a PE router. Traffic coming from the ISPs to the hosts (in the example, traffic traveling from the ISPs on the right to the hosts on the left) is not affected by this feature and does not have to be returned via an MPLS path. This traffic can return via the shortest available IP path.

Another example is a Cable Modem Termination System (CMTS). If the owner of the CMTS wants to allow cable modem subscribers to choose their ISP from a group of ISPs, this feature provides a fast and scalable solution.

## MPLS VPN Traffic Is Unidirectional

In [Figure 1](#), the end users are typical Internet home users. If this were a two-way (bidirectional) feature, traffic coming from the ISPs to the hosts would be required to use only the PE routers that have this feature enabled, which might cause performance issues.

When traffic from the POOL network goes through the Carrier network to the ISP networks for Internet access, the traffic in the Carrier network must be forwarded using MPLS VPN paths, because the router has “selected” the traffic into the correct MPLS VPN.

Traffic from the ISP networks to the POOL network does not have to use MPLS VPN paths in the Carrier network and can use any path that is most efficient to return to the POOL network. This traffic can use a path that uses either MPLS or IP for routing and forwarding and does not have to travel via an MPLS VPN.

Traffic from the ISP networks to the POOL networks can be forwarded using the global routing table used by every interface. One way to accomplish this is to enter VRF static routes on the PE router interfaces connected to the ISPs. The VRF static routes would route traffic from the ISPs to the Carrier network. See the [“Establishing IP Static Routes for a VRF Instance”](#) section on page 11 for information on placing a default VRF static route onto an interface.

Establishing static VRF routes allows traffic from the ISPs to enter the Carrier network as traffic that can only be routed by using the global routing table toward the POOL network.

If the ISPs do not provide global host address space, or this feature is not being used to route Internet traffic, the PE interfaces connected to the ISPs must be placed into a VRF. If the PE interfaces are using VRFs for routing traffic from the ISPs, all traffic from the ISPs to the hosts through the Carrier network would be forwarded using MPLS VPN paths, and performance would not be as optimal as if IP forwarding was used.

Normal IP-based VPN operations, such as populating the Routing Information Base (RIB) and Forwarding Information Base (FIB) from a routing protocol such as Border Gateway Protocol (BGP), are used to route and forward packets within the various VPNs in the customer networks. The provider network uses MPLS-based routing protocols to perform VPN routing and forwarding inside the provider network.

## Conditions That Cause MPLS VPN Traffic To Become Bidirectional

Forwarding of traffic from the Carrier network to the POOL network by using the global routing table is only possible if the ISPs have provided registered IP address space for all of the subscribed users within the POOL network from the global routing table.

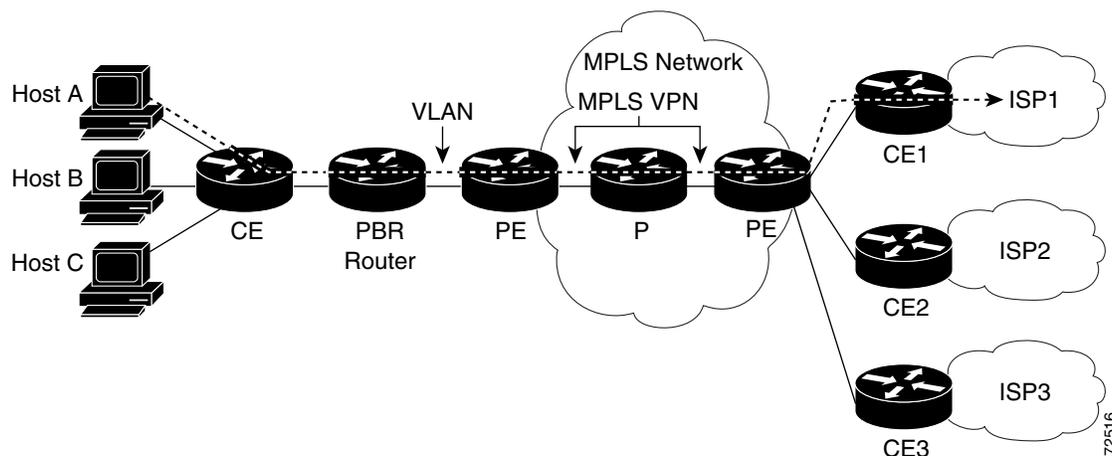
If the POOL network uses IP addresses that are not globally routeable and are designed for a nonconnected enterprise (defined by RFC 1918), this feature becomes bidirectional. All traffic being sent and received by the host would have to travel via a router that has this feature enabled. The POOL network cannot be addressed with overlapping address space, regardless of the type of address space being used.

## Advantages of Using the Source IP Address over Per-Interface IP VPN Configuration

This feature removes the association between a VPN and an interface. Before this feature was introduced, the following implementation was used to route outgoing MPLS VPN packets to different destinations:

- A policy-based router (PBR) is attached to the CE router.
- The egress side of the PBR router side has VLANs connected to a PE.
- The PBR router uses a policy-based route map to select the correct output (VLAN) interface and each VLAN is under a specific VRF. [Figure 2](#) illustrates a sample configuration of using a PBR router for routing MPLS packets to different destinations.

**Figure 2** Implementation of Multiple VPNs



The following limitations apply to PBR-based solutions that use this implementation:

- Policy routing and MPLS VPN functions cannot be performed on the same platform. Integration into a single platform is critical for manageability and support.
- VRF is limited to one VPN per interface, which limits scalability.
- The Cisco 7500 series router is used for the PBR, which can limit network performance.
- There is no network redundancy.
- The PBR is the only point of connection for all the networks attached to the PBR. The capacity and the performance capabilities of the PBR router are critical.
- There is no diversity in the connectivity to the networks.
- Every network is required to connect to every PBR. If every network is not connected to every PBR, packets from the end user to the PBR would be dropped because the PBR would have no way of switching the IP traffic properly.
- Adding multiple PBRs that are interconnected introduces more network policy-routed hops.

This feature addresses the limitations of and problems with using a PBR for packet routing and forwarding.

## Benefits of Directing MPLS VPN Traffic Using a Source IP Address

### **Association of VPN to interface is removed**

This feature removes the association between a VPN and an interface, thus allowing packets from the Host network to the provider network to have more than one VPN available per interface.

### **Access to every customer network is possible from every PE router in the provider network**

Access points to each network can be established at any MPLS PE router, and can be made redundant by connections to multiple PE routers (for example, the CE2 router in [Figure 1 on page 6](#)).

### **Multiple points in the provider network can be used for VPN routing and forwarding**

MPLS VPNs, like IP, are connectionless. Any PE router can carry MPLS VPN traffic from the MPLS network out to the CE routers.

## How to Enable MPLS VPN Traffic To Be Routed Using a Source IP Address

This section includes the following tasks:

- [Enabling Routing of MPLS VPN Traffic Based on the Source IP Address, page 9](#) (required)
- [Establishing IP Static Routes for a VRF Instance, page 11](#) (optional)

## Enabling Routing of MPLS VPN Traffic Based on the Source IP Address

Perform the following steps to enable MPLS VPN traffic to be routed based on the source IP address.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf selection source** *source-IP-address source-IP-mask vrf vrf\_name*
4. **interface** *type number*
5. **ip vrf select source**
6. **ip vrf receive** *vrf\_name*
7. **end**
8. **show ip route vrf**
9. **show ip vrf select**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                 | Enters global configuration mode.                                                                                  |
| Step 3 | <b>vrf selection source</b> <i>source-IP-address source-IP-mask vrf vrf_name</i><br><br><b>Example:</b><br>Router(config)# vrf selection source 16.16.0.0 255.255.0.0 vrf vpn1 | Populates a source IP address to a VRF selection table.                                                            |
| Step 4 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface FastEthernet 0/1                                                                       | Configures an interface and enters interface configuration mode.                                                   |
| Step 5 | <b>ip vrf select source</b><br><br><b>Example:</b><br>Router(config-if)# ip vrf select source                                                                                  | Enables an interface to direct MPLS VPN traffic based on the source IP address of the packet.                      |
| Step 6 | <b>ip vrf receive</b> <i>vrf_name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf receive vpn1                                                                         | Adds all the IP addresses that are associated with an interface into a VRF table.                                  |

|        | Command or Action                                                                                 | Purpose                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Step 7 | <code>end</code><br><br><b>Example:</b><br><code>Router(config-if)# end</code>                    | (Optional) Exits to privileged EXEC mode.                                                                   |
| Step 8 | <code>show ip route vrf</code><br><br><b>Example:</b><br><code>Router# show ip route vrf</code>   | Displays the IP routing table associated with a VRF instance. Use this command to verify the configuration. |
| Step 9 | <code>show ip vrf select</code><br><br><b>Example:</b><br><code>Router# show ip vrf select</code> | Displays information about the VRF selection.                                                               |

## Establishing IP Static Routes for a VRF Instance

Traffic coming from the ISPs to the hosts does not require the use of the MPLS VPN paths; this traffic can use the shortest IP route back to the host.

VPN static routes for traffic returning to the customer networks are only necessary if VPN traffic returning to the customer networks is being forwarded back from the enabled interface. The remote PE router could also be configured to route return traffic to the customer networks directly by using the global routing table.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ip route vrf vrf_name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]`

|        | Command                                                                                           | Purpose                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code> | Enters global configuration mode.                                                                                  |

|        | Command                                                                                                                                                                                                                                 | Purpose                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface FastEthernet 0/1                                                                                                                                | Configures an interface and enters interface configuration mode. |
| Step 4 | <b>ip route vrf</b> <i>vrf_name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]</i><br><br><b>Example:</b><br>Router(config-if)# ip route vrf vpn1 16.16.0.0 255.255.0.0 POS1/0 | Establishes static routes for a VRF.                             |

## Troubleshooting Tips

- Enter the **debug vrf select** command to enable debugging for this feature.



**Note** The **debug vrf select** command can cause many messages to be logged when you change the configuration and when switching occurs.

- The following error messages appear if problems occur while configuring this feature:
  - If you attempt to configure a nonexisting VRF Selection table:
 

```
Router(config)# vrf selection source 2.0.0.0 255.255.0.0 vrf VRF_NOEXIST
VRF Selection: VRF table VRF_NOEXIST does not exist.
```
  - If you attempt to remove a VRF Selection entry that does not exist:
 

```
Router(config)# no vrf selection source 2.0.0.0 255.255.0.0 vrf VRF1
VRF Selection: Can't find the node to remove.
```
  - If you attempt to configure a duplicate IP address and subnet mask for a VRF Selection entry:
 

```
Router(config)# vrf selection source 2.0.0.0 255.0.0.0 vrf VRF_AOL
Router(config)# vrf selection source 2.0.0.0 255.0.0.0 vrf VRF_AOL
VRF Selection: duplicate address and mask configured.
```
  - If an inconsistent IP address and mask are used for a VRF Selection entry:
 

```
Router(config)# vrf selection source 170.1.2.1 255.255.255.0 vrf red
% Inconsistent address and mask
Router(config)# vrf selection source 170.1.2.1 255.255.255.255 vrf red
```
  - If you attempt to configure a VRF instance on an interface that has this feature already configured:
 

```
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf forward red
% Can not configure VRF if VRF Select is already configured
To enable VRF, first remove VRF Select from the interface
```
  - If you attempt to configure an entry on an interface that has this feature already configured:
 

```
Router(config-if)# ip vrf forward red
```

```
Router(config-if)# ip vrf select source
% Can not configure VRF Select if interface is under a non-global VRF
To enable VRF Select, first remove VRF from the interface
```

## Configuration Examples for Directing MPLS VPN Traffic Using a Source IP Address

This section provides the following configuration examples:

- [Enabling MPLS VPN Traffic To Be Routed Based on Source IP Address: Example, page 13](#)
- [Configuring a VRF to Eliminate Unnecessary Packet Forwarding: Example, page 14](#)
- [Verifying the Configuration: Example, page 14](#)

### Enabling MPLS VPN Traffic To Be Routed Based on Source IP Address: Example

The following example defines two entries (vpn1 and vpn2) in the VRF Selection table. In this example, packets with the source address of 16.16.0.0 will be routed to the VRF vpn1, and packets with the source address of 17.17.0.0 will be routed to the VRF vpn2:

```
Router(config)# vrf selection source 16.16.0.0 255.255.0.0 vrf vpn1
Router(config)# vrf selection source 17.17.0.0 255.255.0.0 vrf vpn2
```

The following example creates IP static routes for two VRFs (vpn1 and vpn2) for the POS1/0 interface:

```
Router(config)# ip route vrf vpn1 16.16.0.0 255.255.0.0 POS1/0
Router(config)# ip route vrf vpn2 17.17.0.0 255.255.0.0 POS1/0
```

The following example configures the POS1/0 interface for this feature and adds the configured IP address (31.0.0.1) to the VRFs vpn1 and vpn2 as connected routes.

```
Router(config)# interface POS1/0
Router(config-if)# description Link to CE1 POS1/0 (eng2)
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf receive vpn1
Router(config-if)# ip vrf receive vpn2
Router(config-if)# ip address 31.0.0.1 255.0.0.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# load-interval 30
Router(config-if)# crc 32
Router(config-if)# end
```

## Configuring a VRF to Eliminate Unnecessary Packet Forwarding: Example

If a packet arrives at an interface that has VRF Select enabled, and its source IP address does not match any VRF Select definition, that packet will be forwarded via the global routing table. This default behavior could cause problems if IP address spoofing is being implemented. Unnecessary traffic could be forwarded via the global routing table. To eliminate this unnecessary routing of packets, create a VRF Selection definition that will forward all unknown incoming traffic to a null interface.

The following configuration causes all traffic not matching a more specific VRF Selection definition to be routed to the Null0 interface, thus dropping the packets.

```
Router(config)# ip vrf VRF_DROP
Router(config-vrf)# rd 999:99
Router(config-vrf)# route-target export 999:99
Router(config-vrf)# route-target import 999:99
Router(config-vrf)# exit

Router(config)# vrf selection source 0.0.0.0 0.0.0.0 vrf VRF_DROP

Router(config)# ip route vrf VRF_DROP 0.0.0.0 0.0.0.0 Null0
```

## Verifying the Configuration: Example

This example shows the IP routing table associated with the VRF vrf1:

```
Router# show ip route vrf vpn1
Routing Table: vpn1
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
Gateway of last resort is not set
B 33.0.0.0/8 [200/0] via 10.10.10.10, 00:00:37
 5.0.0.0/16 is subnetted, 1 subnets
B 5.19.0.0 [200/0] via 10.10.10.10, 00:00:37
 14.0.0.0/32 is subnetted, 1 subnets
B 14.14.14.14 [200/0] via 10.10.10.10, 00:00:37
 15.0.0.0/32 is subnetted, 1 subnets
S 15.15.15.15 [1/0] via 34.0.0.1, POS1/1
```

## Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic MPLS VPNs                     | <a href="#">Configuring MPLS Layer 3 VPNs</a><br><a href="#">Configuring Scalable Hub-and-Spoke MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a></li> <li>• <a href="#">Preserving QoS Settings in an MPLS VPN Carrier Supporting Carrier Network</a></li> <li>• <a href="#">Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</a></li> </ul> |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> </ul>                                                                                                                                                                                                          |
| MPLS VPN route maps                 | <a href="#">Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MPLS VPN load sharing               | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN MIBs                       | <a href="#">Monitoring MPLS VPNs with MIBs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Directing MPLS VPN traffic          | <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| VPN ID                              | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Dialer applications with MPLS VPNs  | <a href="#">Dialing to Destinations with the Same IP Address for MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MPLS VPNs and OSPF                  | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Directing MPLS VPN Traffic Using a Source IP Address

Table 1 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Directing MPLS VPN Traffic Using a Source IP Address

| Feature Name                             | Releases                                         | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VRF Selection Based on Source IP Address | 12.0(22)S<br>12.0(23)S<br>12.0(24)S<br>12.0(26)S | <p>This feature lets you direct MPLS VPN traffic based on the source IP address of the packet.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Introduction to Directing MPLS VPN Traffic Using a Source IP Address, page 4</a></li> <li>• <a href="#">How MPLS VPN Traffic Is Routed Using the Source IP Address, page 4</a></li> <li>• <a href="#">Example of MPLS VPN Traffic Being Routed Based on the Source IP Address, page 5</a></li> <li>• <a href="#">Advantages of Using the Source IP Address over Per-Interface IP VPN Configuration, page 8</a></li> <li>• <a href="#">Benefits of Directing MPLS VPN Traffic Using a Source IP Address, page 9</a></li> <li>• <a href="#">How to Enable MPLS VPN Traffic To Be Routed Using a Source IP Address, page 9</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.





## Monitoring MPLS VPNs with MIBs

---

This module explains how to use the PPVPN-MPLS-VPN management information base (MIB) to monitor and manage Multiprotocol Label Switching (MPLS) Virtual Private Networks. The following MIBs are supported:

- *MPLS/BGP Virtual Private Network Management Information Base Using SMIPv2 (draft-ietf-ppvpn-mpls-vpn-mib-03.txt)*
- CISCO-IETF-PPVPN-MPLS-VPN-MIB, a proprietary MIB that describes the cMplsNumVrfRouteMaxThreshCleared notification

### Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

### Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for PPVPN MPLS VPN MIB”](#) section on page 31.

## Contents

- [Prerequisites for PPVPN MPLS VPN MIB, page 2](#)
- [Restrictions for PPVPN MPLS VPN MIB, page 2](#)
- [Information About PPVPN MPLS VPN MIB, page 2](#)
- [How to Configure PPVPN MPLS VPN MIB, page 21](#)
- [Configuration Examples for PPVPN MPLS VPN MIB, page 27](#)
- [Additional References, page 29](#)
- [Feature Information for PPVPN MPLS VPN MIB, page 31](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for PPVPN MPLS VPN MIB

The PPVPN-MPLS-VPN MIB agent requires the following:

- SNMP is installed and enabled on the label switching routers.
- MPLS is enabled on the label switching routers.
- Multiprotocol Border Gateway Protocol (BGP) is enabled on the label switching routers.
- Cisco Express Forwarding is enabled on the label switching routers.

## Restrictions for PPVPN MPLS VPN MIB

The following restrictions apply to the PPVPN-MPLS-VPN MIB:

- Configuration of the MIB using the SNMP SET command is not supported, except for trap-related objects, such as `mplsVpnNotificationEnable` and `mplsVpnVrfSecIllegalLabelRcvThresh`.
- The `mplsVpnVrfBgpNbrPrefixTable` is not supported.

## Information About PPVPN MPLS VPN MIB

This section contains the following topics:

- [MPLS VPN Overview, page 2](#)
- [PPVPN MPLS VPN MIB Overview, page 3](#)
- [PPVPN MPLS VPN MIB and the IETF, page 3](#)
- [Capabilities Supported by PPVPN-MPLS-VPN MIB, page 4](#)
- [Functional Structure of the PPVPN-MPLS-VPN MIB, page 4](#)
- [Supported Objects in PPVPN-MPLS-VPN MIB, page 4](#)
- [MIB Objects Not Supported, page 20](#)

## MPLS VPN Overview

The MPLS VPN technology allows service providers to offer intranet and extranet VPN services that directly connect their customers' remote offices to a public network with the same security and service levels that a private network offers. Each VPN is associated with one or more VPN routing/forwarding instances (VRFs). A VRF is created for each VPN defined on a router and contains most of the information needed to manage and monitor MPLS VPNs: an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use this forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

## PPVPN MPLS VPN MIB Overview

The Provider-Provisioned VPN (PPVPN)-MPLS-VPN MIB provides access to VRF information, as well as interfaces included in the VRF, and other configuration and monitoring information.

The PPVPN-MPLS-VPN MIB provides the following benefits:

- A standards-based SNMP interface for retrieving information about critical MPLS VPN events.
- VRF information to assist in the management and monitoring of MPLS VPNs.
- Information, in conjunction with the Interfaces MIB, about interfaces assigned to VRFs.
- Performance statistics for all VRFs on a router.
- The generation and queuing of notifications that call attention to major changes in the operational status of MPLS VPN enabled interfaces; the forwarding of notification messages to a designated network management system (NMS) for evaluation and action by network administrators.
- Advanced warning when VPN routing tables are approaching or exceed their capacity.
- Warnings about the reception of illegal labels on a VRF-enabled interface. Such receptions may indicate misconfiguration or an attempt to violate security.

This document also describes the CISCO-IETF-PPVPN-MPLS-VPN-MIB, which contains the `cMplsNumVrfRouteMaxThreshCleared` notification.

## PPVPN MPLS VPN MIB and the IETF

SNMP agent code operating with the PPVPN-MPLS-VPN MIB enables a standardized, SNMP-based approach to managing MPLS VPNs in Cisco IOS software.

The PPVPN-MPLS-VPN MIB is based on the IETF draft MIB specification *draft-ietf-ppvpn-mpls-vpn-mib-03.txt*, which includes objects describing features that support MPLS VPN events. This IETF draft MIB, which undergoes revisions from time to time, is being evolved toward becoming a standard. Accordingly, the Cisco implementation of the PPVPN-MPLS-VPN MIB is expected to track the evolution of the IETF draft MIB, and may change accordingly.

Some slight differences between the IETF draft MIB and the actual implementation of MPLS VPNs within Cisco IOS software require some minor translations between the PPVPN-MPLS-VPN MIB and the internal data structures of Cisco IOS. These translations are accomplished by means of the SNMP agent code. Also, while running as a low priority process, the SNMP agent provides a management interface to Cisco IOS. SNMP adds little overhead on the normal functions of the device.

The SNMP objects defined in the PPVPN-MPLS-VPN MIB can be viewed by any standard SNMP utility. The network administrator can retrieve information in the PPVPN-MPLS-VPN MIB using standard SNMP **get** and **getnext** operations for SNMP v1, v2, and v3.

All PPVPN-MPLS-VPN MIB objects are based on the IETF draft MIB; thus, no Cisco specific SNMP application is required to support the functions and operations pertaining to the PPVPN-MPLS-VPN MIB features.

## Capabilities Supported by PPVPN-MPLS-VPN MIB

The following functionality is supported by the PPVPN-MPLS-VPN MIB. The PPVPN-MPLS-VPN MIB provides you with the ability to do the following:

- Gather routing and forwarding information for MPLS VPNs on a router.
- Expose information in the VRF routing table.
- Gather information on BGP configuration related to VPNs and VRF interfaces and statistics.
- Emit notification messages that signal changes when critical MPLS VPN events occur.
- Enable, disable, and configure notification messages for MPLS VPN events by using extensions to existing SNMP CLI commands.
- Specify the IP address of a network management system (NMS) in the operating environment to which notification messages are sent.
- Write notification configurations into nonvolatile memory.

## Functional Structure of the PPVPN-MPLS-VPN MIB

The SNMP agent code supporting the PPVPN-MPLS-VPN MIB follows the existing model for such code in Cisco IOS software and is, in part, generated by the Cisco IOS tool set, based on the MIB source code.

The SNMP agent code, which has a layered structure that is common to MIB support code in Cisco IOS, consists of four layers:

- Platform-independent layer—This layer is generated primarily by the MIB development Cisco IOS tool set and incorporates platform- and implementation-independent functions. The Cisco IOS MIB development tool set creates a standard set of files associated with a MIB.
- Application interface layer—The functions, names, and template code for MIB objects in this layer are also generated by the MIB development Cisco IOS tool set.
- Application-specific layer—This layer provides an interface between the application interface layer and the API and data structures layer below and performs tasks needed to retrieve required information from Cisco IOS, such as searching through data structures.
- API and data structures layer—This layer contains the data structures or APIs within Cisco IOS that are retrieved or called in order to set or retrieve SNMP management information.

## Supported Objects in PPVPN-MPLS-VPN MIB

The PPVPN-MPLS-VPN MIB contains numerous tables and object definitions that provide read-only SNMP management support for the MPLS VPN feature in Cisco IOS. The PPVPN-MPLS-VPN MIB conforms to Abstract Syntax Notation One (ASN.1), thus reflecting an idealized MPLS VPN database.

Using any standard SNMP network management application, you can retrieve and display information from the PPVPN-MPLS-VPN MIB using GET operations; similarly, you can traverse information in the MIB database for display using GETNEXT operations.

The PPVPN-MPLS-VPN MIB tables and objects are described briefly in the following sections:

- [Scalar Objects, page 5](#)
- [MIB Tables, page 6](#)

- [Notifications, page 17](#)

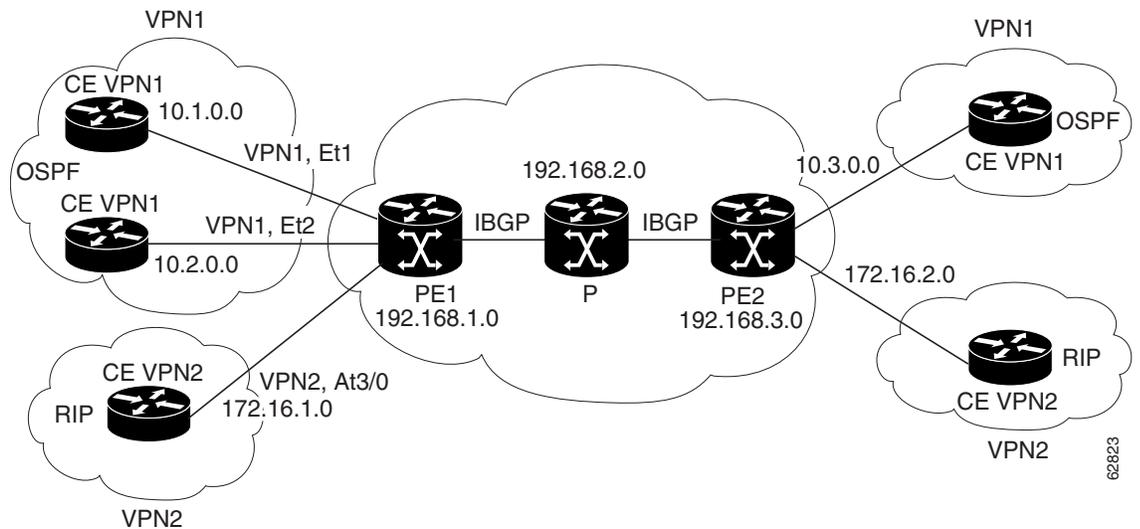
Objects that are not supported are listed in the “[MIB Objects Not Supported](#)” section on page 20.

[Figure 1](#) shows a simple MPLS VPN configuration. This configuration includes two customer MPLS VPNs, labeled VPN1 and VPN2, and a simple provider network that consists of two provider edge (PE) routers, labeled PE1 and PE2, and a provider core router labeled P. [Figure 1](#) shows the following sample configuration:

- VRF names—VPN1 and VPN2
- Interfaces associated with VRFs—Et1, Et2, and At3/0
- Routing protocols—OSPF, RIP, and IBGP
- Routes associated with VPN1—10.1.0.0, 10.2.0.0, and 10.3.0.0
- Routes associated with VPN2—172.16.1.0 and 172.16.2.0
- Routes associated with the provider network—192.168.1.0, 192.168.2.0, and 192.168.3.0

This configuration is used in this document to explain MPLS VPN events that are monitored and managed by the PPVPN-MPLS-VPN MIB.

**Figure 1** Sample MPLS VPN Configuration



## Scalar Objects

[Table 1](#) shows the supported PPVPN-MPLS-VPN MIB scalar objects.

**Table 1** PPVPN-MPLS-VPN MIB Scalar Objects

| MIB Object            | Function                                                                                                                                     |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| mplsVpnConfiguredVrfs | The number of VRFs configured on the router, including VRFs recently deleted.                                                                |
| mplsVpnActiveVrfs     | The number of VRFs that are active on the router. An active VRF is assigned to at least one interface that is in the operationally up state. |

**Table 1** *PPVPN-MPLS-VPN MIB Scalar Objects (continued)*

| MIB Object                      | Function                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsVpnConnectedInterfaces      | The total number of interfaces assigned to any VRF.                                                                                                                                                                                                                                                                                                                            |
| mplsVpnNotificationEnable       | <p>A value that indicates whether all the PPVPN-MPLS-VPN MIB notifications are enabled.</p> <ul style="list-style-type: none"> <li>• Setting this object to true enables all notifications defined in the PPVPN-MPLS-VPN MIB.</li> <li>• Setting it to false disables all notifications defined in the MIB.</li> </ul> <p>This is one of the few objects that is writable.</p> |
| mplsVpnVrfConfMaxPossibleRoutes | A number that indicates the amount of routes that this router is capable of storing. This value cannot be determined because it is based on the amount of available memory in the system. Therefore, this object is set to zero (0).                                                                                                                                           |

## MIB Tables

The PPVPN-MPLS-VPN MIB implementation supports the following tables described in this section:

- [mplsVpnVrfTable](#), page 7
- [mplsVpnInterfaceConfTable](#), page 8
- [mplsVpnVrfRouteTargetTable](#), page 10
- [mplsVpnVrfBgpNbrAddrTable](#), page 12
- [mplsVpnVrfSecTable](#), page 13
- [mplsVpnVrfPerfTable](#), page 13
- [mplsVpnVrfRouteTable](#), page 14

## mplsVpnVrfTable

Entries in the VRF configuration table (mplsVpnVrfTable) represent the VRFs that are defined on the router. This includes recently deleted VRFs. The information in this table is also displayed with the **show ip vrf** command.

Each VRF is referenced by its VRF name (mplsVpnVrfName).

Table 2 lists the MIB objects and their functions for this table.

**Table 2** PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfTable

| MIB Object                      | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsVpnVrfName                  | The name associated with this VRF. When this object is used as an index to a table, the first octet is the string length, and subsequent octets are the ASCII codes of each character. For example, "vpn1" is represented as 4.118.112.110.49.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| mplsVpnVrfDescription           | The description of the VRF. This is specified with the following configuration command:<br><br><pre>Router(config)# ip vrf vrf-name Router(config-vrf)# description vrf-description</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| mplsVpnVrfRouteDistinguisher    | The route distinguisher for this VRF. This is specified with the following configuration command:<br><br><pre>Router(config)# ip vrf vrf-name Router(config-vrf)# rd route-distinguisher</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| mplsVpnVrfCreationTime          | The value of the sysUpTime when this VRF entry was created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| mplsVpnVrfOperStatus            | The operational status of this VRF. A VRF is up (1) when at least one interface associated with the VRF is up. A VRF is down (2) when: <ul style="list-style-type: none"> <li>• No interfaces exist whose ifOperStatus = up (1).</li> <li>• No interfaces are associated with this VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| mplsVpnVrfActiveInterfaces      | The number of interfaces assigned to this VRF which are operationally up.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| mplsVpnVrfAssociatedInterfaces  | The number of interfaces assigned to this VRF, independent of the operational status.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| mplsVpnVrfConfMidRouteThreshold | The middle route threshold. If the amount of routes in the VRF crosses this threshold, an mplsNumVrfRouteMidThreshExceeded notification is sent (if notifications are enabled and configured). You can set this value in configuration mode as a percentage of the maximum with the <b>maximum routes limit {warn-threshold   warn-only}</b> command, as follows:<br><br><pre>Router(config)# ip vrf vpn1 Router(config-vrf)# maximum routes 1000 50</pre> <p>The middle or warn threshold is set for VRF vpn1 as 50% of the maximum route threshold.</p> <p>The following command sets a middle threshold of 1000 routes. An mplsNumVrfRouteMidThreshExceeded notification is sent when this threshold is exceeded. However, additional routes are still allowed because a maximum route threshold is not set with this command.</p> <pre>Router(config-vrf)# maximum routes 1000 warn-only</pre> |

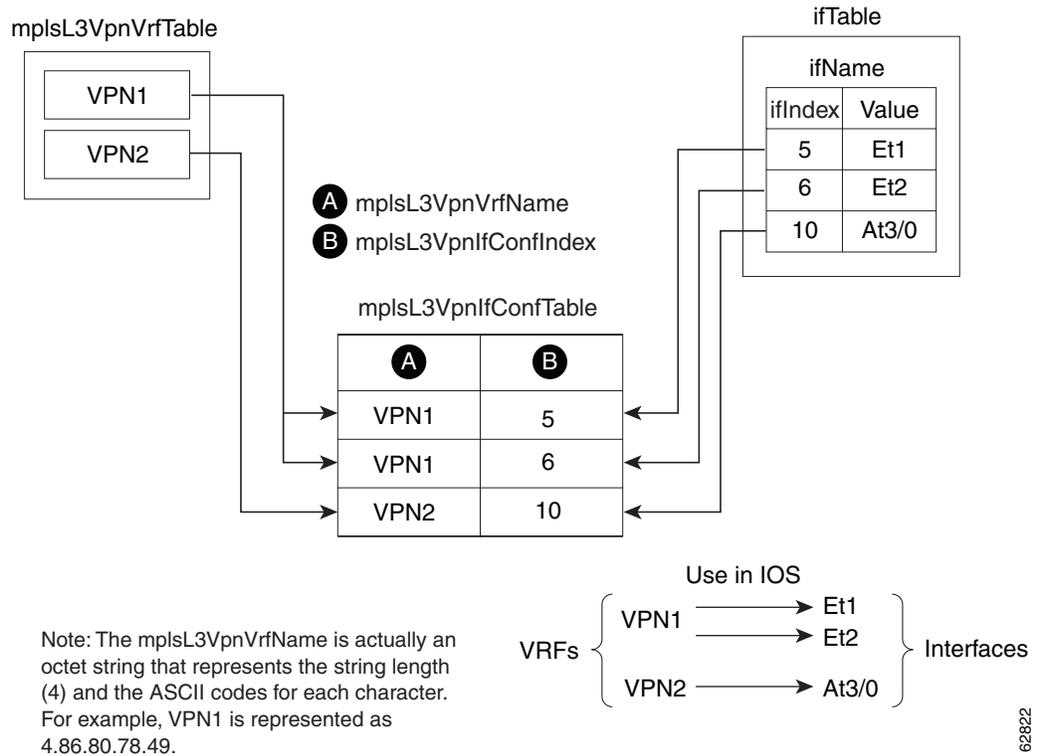
Table 2 PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfTable (continued)

| MIB Object                       | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsVpnVrfConfHighRouteThreshold | <p>The maximum route threshold. If the amount of routes in the VRF crosses this threshold, an mplsNumVrfRouteMaxThreshExceeded notification is sent (if notifications are enabled and configured). You can set this value in configuration mode with the <b>maximum routes limit {warn-threshold   warn-only}</b> command as follows:</p> <pre>Router(config)# ip vrf vpn2</pre> <pre>Router(config-vrf)# maximum routes 1000 75</pre> <p>The maximum route threshold is set for 1000 routes for VRF vpn2 with a middle or warn threshold of 75% of this threshold.</p> |
| mplsVpnVrfConfMaxRoutes          | This value is the same as the mplsVpnVrfConfHighRouteThreshold.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| mplsVpnVrfConfLastChanged        | <p>The value of sysUpTime when the configuration of the VRF changes or interfaces are assigned or unassigned from the VRF.</p> <p><b>Note</b> This object is updated only when values in this table change.</p>                                                                                                                                                                                                                                                                                                                                                         |
| mplsVpnVrfConfRowStatus          | Read-only implementation. This object normally reads “active (1),” but may read “notInService (2),” if a VRF was recently deleted.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| mplsVpnVrfConfStorageType        | Read-only implementation. This object always reads “volatile (2).”                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

### mplsVpnInterfaceConfTable

In Cisco IOS, a VRF is associated with one MPLS VPN. Zero or more interfaces can be associated with a VRF. A VRF uses an interface that is defined in the ifTable of the Interfaces Group of MIB II (IFMIB). The IFMIB defines objects for managing interfaces. The ifTable of this MIB contains information on each interface in the network. The mplsVpnInterfaceConfTable associates a VRF from the mplsVpnVrfTable with a forwarding interface from the ifTable. [Figure 2](#) shows the relationship between VRFs and interfaces defined in the ifTable and the mplsVpnInterfaceConfTable.

**Figure 2** VRFs, the Interfaces MIB, and the *mplsVpnInterfaceConfTable*



Entries in the VPN interface configuration table (*mplsVpnInterfaceConfTable*) represent the interfaces that are assigned to each VRF. The information available in this table is also displayed with the **show ip vrf** command.

The *mplsVpnInterfaceConfTable* shows how interfaces are assigned to VRFs. A label switch router (LSR) creates an entry in this table for every interface capable of supporting MPLS VPNs.

The `mplsVpnInterfaceConfTable` is indexed by the following:

- `mplsVpnVrfName`—The VRF name
- `mplsVpnInterfaceConfIndex`—An identifier that is the same as the `ifIndex` from the Interface MIB of the interface assigned to the VRF

Table 3 lists the MIB objects and their functions for this table.

**Table 3** PPVPN-MPLS-VPN MIB Objects for the `mplsVpnInterfaceConfTable`

| MIB Object                                        | Function                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>mplsVpnInterfaceConfIndex</code>            | Provides the interface MIB <code>ifIndex</code> of this interface that is assigned to a VRF.                                                                                                                                                                                                                                                        |
| <code>mplsVpnInterfaceLabelEdgeType</code>        | Indicates whether the interface is a provider edge interface (1) or a customer edge interface (2).<br><br>This value is always <code>providerEdge</code> (1) because in Cisco IOS, <code>customerEdge</code> interfaces are not assigned to VRFs and do not appear in this table.                                                                   |
| <code>mplsVpnInterfaceVpnClassification</code>    | Specifies what type of VPN this interface is providing: carrier supporting carrier (CsC) (1), enterprise (2), or InterProvider (3).<br><br>This value is set to <code>enterprise</code> (2) if MPLS is not enabled and to <code>carrier supporting carrier</code> (1) if MPLS is enabled on this interface.                                         |
| <code>mplsVpnInterfaceVpnRouteDistProtocol</code> | Indicates the route distribution protocols that are being used to redistribute routes with BGP on this interface: BGP (2), OSPF (3), or RIP (4).<br><br>In Cisco IOS, router processes are defined and redistributed on a per-VRF basis, not per-interface. Therefore, all interfaces assigned to the same VRF have the same value for this object. |
| <code>mplsVpnInterfaceConfStorageType</code>      | Read-only implementation. This object always reads “ <code>volatile</code> (2).”                                                                                                                                                                                                                                                                    |
| <code>mplsVpnInterfaceConfRowStatus</code>        | Read-only implementation. This object normally reads “ <code>active</code> (1),” but may read “ <code>notInService</code> (2),” if a VRF was recently deleted.                                                                                                                                                                                      |

### `mplsVpnVrfRouteTargetTable`

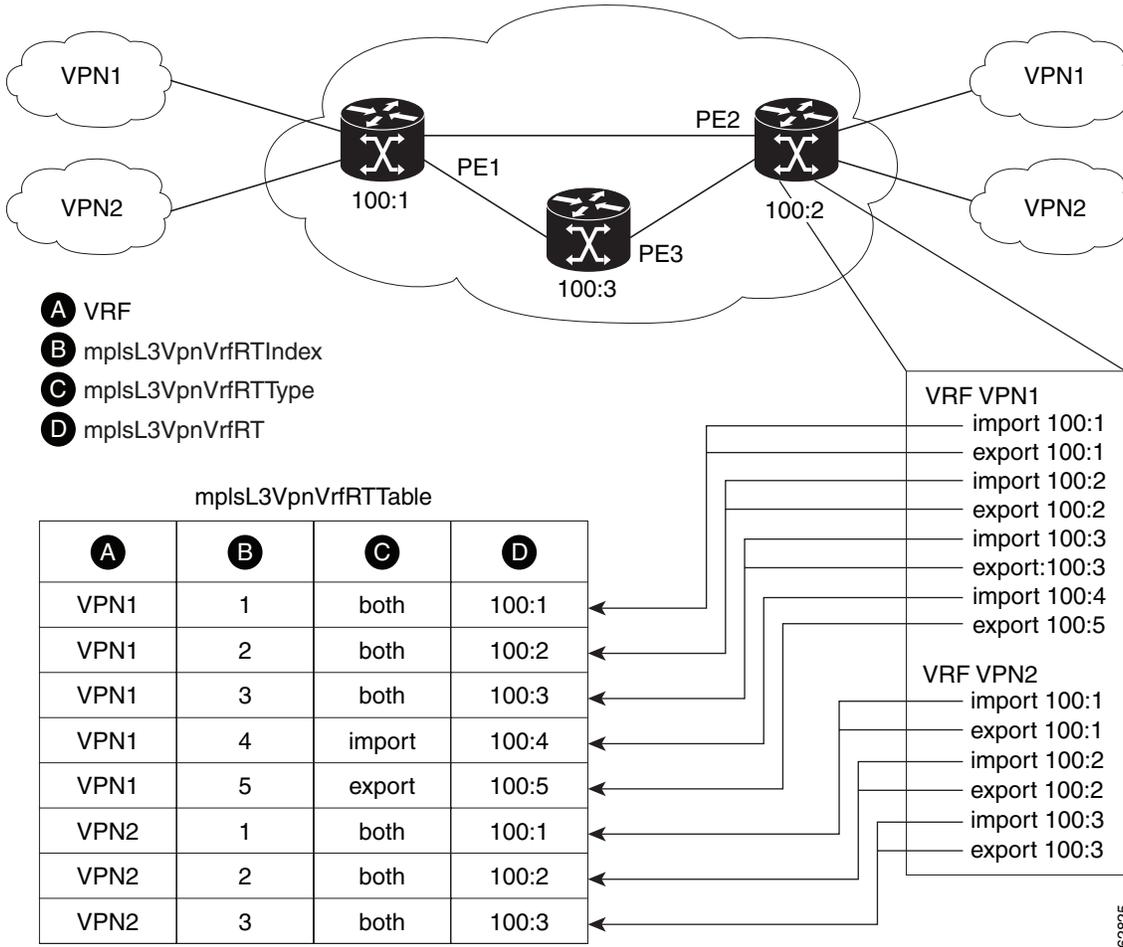
The route target table (`mplsVpnVrfRouteTargetTable`) describes the route target communities that are defined for a particular VRF. An LSR creates an entry in this table for each target configured for a VRF supporting an MPLS VPN instance.

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by Border Gateway Protocol (BGP) extended communities. Distribution of VPN routing information works as follows:

- When a VPN route learned from a CE router is injected into BGP, a list of VPN route target extended community attributes are associated with it. Typically the list of route target community values is set from an export list of route targets associated with the VRF from which the route was learned.
- An import list of route target extended communities is associated with each VRF. The import list defines route target extended community attributes a route must have for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target communities A, B, and C, then any VPN route that carries any of those route target extended communities—A, B, or C—is imported into the VRF.

Figure 3 shows a sample configuration and its relationship to an mplsVpnVrfRouteTargetTable. A route target table exists on each PE router. Routers with route distinguishers (RDs) 100:1, 100:2, and 100:3 are shown in the sample configuration. Routers with RDs 100:4 and 100:5 are not shown in Figure 3, but are included in the route targets for PE2 and in the mplsVpnVrfRouteTargetTable.

Figure 3 Sample Configuration and the mplsVpnVrfRouteTargetTable



Note: The mplsL3VpnVrfName is actually an octet string that represents the string length (4) and the ASCII codes for each character. For example, VPN1 is represented as 4.86.80.78.49.

The `mplsVpnVrfRouteTargetTable` shows the import and export route targets for each VRF. The table is indexed by the following:

- `mplsVpnVrfName`—The VRF name
- `mplsVpnVrfRouteTargetIndex`—The route target entry identifier
- `mplsVpnVrfRouteTargetType`—A value specifying whether the entry is an import route target, export route target, or is defined as both

Table 4 lists the MIB objects and their functions for this table.

**Table 4** PPVPN-MPLS-VPN MIB Objects for the `mplsVpnVrfRouteTargetTable`

| MIB Object                                  | Function                                                                                                                                 |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <code>mplsVpnVrfRouteTargetIndex</code>     | A value that defines each route target's position in the table.                                                                          |
| <code>mplsVpnVrfRouteTargetType</code>      | Determines which type of route target the entry represents: import (1), export (2), or both (3).                                         |
| <code>mplsVpnVrfRouteTarget</code>          | Determines the route distinguisher for this target.                                                                                      |
| <code>mplsVpnVrfRouteTargetDescr</code>     | Description of the route target. This object is not supported. Therefore, the object is the same as <code>mplsVpnVrfRouteTarget</code> . |
| <code>mplsVpnVrfRouteTargetRowStatus</code> | Read-only implementation. This object normally reads "active (1)," but may read "notInService (2)," if a VRF was recently deleted.       |

### `mplsVpnVrfBgpNbrAddrTable`

The BGP neighbor address table (`mplsVpnVrfBgpNbrAddrTable`) represents the MPLS eBGP neighbors that are defined for a particular VRF. An LSR creates an entry for every BGP neighbor that is defined in the VRF's address-family.

The `mplsVpnVrfBgpNbrAddrTable` is indexed by the following:

- `mplsVpnVrfName`—The VRF name
- `mplsVpnInterfaceConfIndex`—An identifier that is the same as the `ifIndex` from the Interface MIB of the interface assigned to the VRF
- `mplsVpnVrfBgpNbrIndex`—The IP address of the neighbor

Table 5 lists the MIB objects and their functions for this table.

**Table 5** PPVPN-MPLS-VPN MIB Objects for the `mplsVpnVrfBgpNbrAddrTable`

| MIB Object                               | Function                                                                                                                                                                                                                                                    |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>mplsVpnVrfBgpNbrIndex</code>       | The IPv4 address of the eBGP neighbor.                                                                                                                                                                                                                      |
| <code>mplsVpnVrfBgpNbrRole</code>        | The role of this eBGP neighbor: customer edge (1) or provider edge (2). If the object <code>mplsVpnInterfaceVpnClassification</code> is carrier supporting carrier (CSC), then this value is provider edge (2), otherwise, this value is customer edge (1). |
| <code>mplsVpnVrfBgpNbrType</code>        | Address type of this eBGP neighbor. The MIB only supports IPv4 (1). Therefore, this object returns "ipv4 (1)."                                                                                                                                              |
| <code>mplsVpnVrfBgpNbrAddr</code>        | IP address of the eBGP neighbor.                                                                                                                                                                                                                            |
| <code>mplsVpnVrfBgpNbrRowStatus</code>   | Read-only implementation. This object normally reads "active (1)," but may read "notInService (2)" if a VRF was recently deleted.                                                                                                                           |
| <code>mplsVpnVrfBgpNbrStorageType</code> | Read-only implementation. This object always reads "volatile (2)."                                                                                                                                                                                          |

## mplsVpnVrfSecTable

The VRF security table (mplsVpnVrfSecTable) provides information about security for each VRF. An LSR creates an entry in this table for every VRF capable of supporting MPLS VPN.

The mplsVpnVrfSecTable *augments* the mplsVpnVrfTable and has the same indexing.

Table 6 lists the MIB objects and their functions for this table.

**Table 6** PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfSecTable

| MIB Object                          | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mplsVpnVrfSecIllegalLabelViolations | <p>The number of illegally received labels on a VRF interface. Only illegal labels are counted by this object, therefore the object only applies to a VRF interface that is MPLS enabled (carrier supporting carrier [CsC] situation).</p> <p>This counter is incremented whenever a label is received that is above or below the valid label range, not in the global label forwarding table, or is received on the wrong VRF (that is, table IDs for the receiving interface and appropriate VRF label forwarding table do not match).</p> |
| mplsVpnVrfSecIllegalLabelRcvThresh  | <p>Notification threshold for illegal labels received on this VRF. When the amount of illegal labels received on this interface crosses this threshold, an mplsNumVrfSecIllegalLabelThreshExceeded notification is sent (if the notification is enabled and configured).</p> <p>This object is one of the few in this MIB agent that supports the SNMP SET operation, which allows you to change this value.</p>                                                                                                                             |

## mplsVpnVrfPerfTable

The VRF performance table (mplsVpnVrfPerfTable) provides statistical performance information for each VRF. An LSR creates an entry in this table for every VRF capable of supporting MPLS VPN.

The mplsVpnVrfPerfTable *augments* the mplsVpnVrfTable and has the same indexing.

Table 7 lists the MIB objects and their functions for this table.

**Table 7** PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfPerfTable

| MIB Objects                 | Functions                                                               |
|-----------------------------|-------------------------------------------------------------------------|
| mplsVpnVrfPerfRoutesAdded   | The number of routes added to this VRF over the course of its lifetime. |
| mplsVpnVrfPerfRoutesDeleted | The number of routes removed from this VRF.                             |
| mplsVpnVrfPerfCurrNumRoutes | The number of routes currently defined within this VRF.                 |

## mplsVpnVrfRouteTable

The VRF routing table (mplsVpnVrfRouteTable) provides the IP routing table information for each VRF. The information available in this table can also be accessed with the **show ip route vrf vrf-name** command. For example, for PE1 in [Figure 1](#):

- With the **show ip route vrf vpn1** command, you would see results like the following:

```
Router# show ip route vrf vpn1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
!
Gateway of last resort is not set
!
 10.0.0.0/32 is subnetted, 3 subnets
B 10.3.0.0 [200/0] via 192.168.2.1, 04:36:33
C 10.1.0.0/16 is directly connected, Ethernet1
C 10.2.0.0/16 [200/0] directly connected Ethernet2, 04:36:33
```

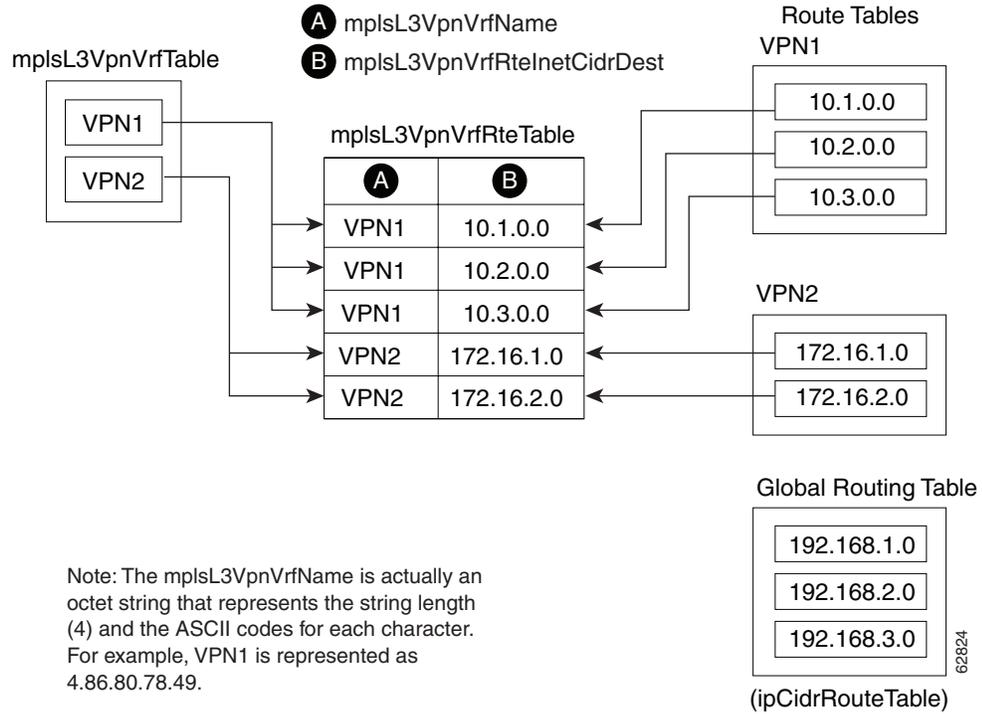
- With the **show ip route vrf vpn2** command, you would see results like the following:

```
Router# show ip route vrf vpn2

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
!
Gateway of last resort is not set
!
 172.16.0.0/32 is subnetted, 2 subnets
B 172.16.2.0 [200/0] via 192.168.2.1, 04:36:33
C 172.16.1.0 is directly connected, ATM 3/0
```

Figure 4 shows the relationship of the routing tables, the VRFs, and the `mplsVpnVrfRouteTable`. You can view information about the VPN1 and VPN2 route tables using the `show ip route vrf vrf-name` command. The global route table is the same as `ipCidrRouteTable` in the IP-FORWARD-MIB. You can view information about the global route table with the `show ip route` command.

**Figure 4** Route Table, VRFs, and the `mplsVpnVrfRouteTable`



An LSR creates an entry in this table for every route that is configured, either dynamically or statically, within the context of a specific VRF capable of supporting MPLS VPN.

The `mplsVpnVrfRouteTable` is indexed by the following:

- `mplsVpnVrfName`—The VRF name, which provides the VRF routing context
- `mplsVpnVrfRouteDest`—The IP destination address
- `mplsVpnVrfRouteMask`—The IP destination mask
- `mplsVpnVrfRouteTos`—The IP header ToS bits
- `mplsVpnVrfRouteNextHop`—The IP address of the next hop for each route entry

**Note**

The ToS bits are not supported and, therefore, are always 0.

[Table 8](#) lists the MIB objects and their functions for the `mplsVpnVrfRouteTable`. This table represents VRF-specific routes. The global routing table is the `ipCidrRouteTable` in the IP-FORWARD-MIB.

**Table 8** PPVPN-MPLS-VPN MIB Objects for the `mplsVpnVrfRouteTable`

| MIB Object                                                                                                                                               | Function                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>mplsVpnVrfRouteDest</code>                                                                                                                         | The destination IP address defined for this route.                                                                                                                                                                     |
| <code>mplsVpnVrfRouteDestAddrType</code>                                                                                                                 | The address type of the IP destination address ( <code>mplsVpnVrfRouteDest</code> ). This MIB implementation only supports IPv4 (1). Therefore, this object has a value of “ipv4 (1).”                                 |
| <code>mplsVpnVrfRouteMask</code>                                                                                                                         | The destination IP address mask defined for this route.                                                                                                                                                                |
| <code>mplsVpnVrfRouteMaskAddrType</code>                                                                                                                 | The address type of the destination IP address mask. This MIB implementation only supports IPv4 (1). Therefore, this object has a value of “ipv4 (1).”                                                                 |
| <code>mplsVpnVrfRouteTos</code>                                                                                                                          | The ToS bits from the IP header for this route. Cisco IOS software only supports ToS bits of zero. Therefore, the object is always 0.                                                                                  |
| <code>mplsVpnVrfRouteNextHop</code>                                                                                                                      | The next hop IP address defined for this route.                                                                                                                                                                        |
| <code>mplsVpnVrfRouteNextHopAddrType</code>                                                                                                              | The address type of the next hop IP address. This MIB implementation only supports IPv4 (1). Therefore, this object has a value of “ipv4 (1).”                                                                         |
| <code>mplsVpnVrfRouteIfIndex</code>                                                                                                                      | The interface MIB <code>ifIndex</code> for the interface through which this route is forwarded. The object is 0 if no interface is defined for the route.                                                              |
| <code>mplsVpnVrfRouteType</code>                                                                                                                         | Defines if this route is a local or remotely defined route.                                                                                                                                                            |
| <code>mplsVpnVrfRouteProto</code>                                                                                                                        | The routing protocol that was responsible for adding this route to the VRF.                                                                                                                                            |
| <code>mplsVpnVrfRouteAge</code>                                                                                                                          | The number of seconds since this route was last updated.                                                                                                                                                               |
| <code>mplsVpnVrfRouteInfo</code>                                                                                                                         | A pointer to more information from other MIBs. This object is not supported and always returns “nulloid (0.0).”                                                                                                        |
| <code>mplsVpnVrfRouteNextHopAS</code>                                                                                                                    | The autonomous system number of the next hop for this route. This object is not supported and is always 0.                                                                                                             |
| <code>mplsVpnVrfRouteMetric1</code>                                                                                                                      | The primary routing metric used for this route.                                                                                                                                                                        |
| <code>mplsVpnVrfRouteMetric2</code><br><code>mplsVpnVrfRouteMetric3</code><br><code>mplsVpnVrfRouteMetric4</code><br><code>mplsVpnVrfRouteMetric5</code> | Alternate routing metrics used for this route. These objects are supported only for Cisco IGRP and Cisco EIGRP. These objects display the bandwidth metrics used for the route. Otherwise, these values are set to -1. |

**Table 8** PPVPN-MPLS-VPN MIB Objects for the *mplsVpnVrfRouteTable* (continued)

| MIB Object                        | Function                                                                                                                           |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <i>mplsVpnVrfRouteRowStatus</i>   | Read-only implementation. This object normally reads “active (1),” but may read “notInService (2),” if a VRF was recently deleted. |
| <i>mplsVpnVrfRouteStorageType</i> | Read-only implementation. This object always reads “volatile (2).”                                                                 |

## Notifications

This section provides the following information about supported PPVPN-MPLS-VPN MIB notifications:

- [PPVPN-MPLS-VPN MIB Notification Events, page 17](#)
- [Notification Specification, page 20](#)
- [Monitoring the PPVPN-MPLS-VPN MIB Notifications, page 20](#)

### PPVPN-MPLS-VPN MIB Notification Events

The following notifications of the PPVPN-MPLS-VPN MIB are supported:

- **mplsVrffUp**—Sent to an NMS when an interface comes up and is assigned a VPN routing/forwarding table instance (VRF).
- **mplsVrffDown**—Generated and sent to the NMS when a VRF is removed from an interface or the interface transitions from an operationally “up” state to a “down” state.
- **mplsNumVrfRouteMidThreshExceeded**—Generated and sent when the middle (warning) threshold is crossed. You can configure this threshold in the CLI by using the following commands:

```
Router(config)# ip vrf vrf-name
```

```
Router(config-vrf)# maximum routes limit warn-threshold (% of max)
```

The *warn-threshold* argument is a percentage of the maximum routes specified by the *limit* argument. You can also configure a middle threshold with the following command, in which the *limit* argument represents the warning threshold:

```
Router(config-vrf)# maximum routes limit warn-only
```

This notification is sent to the NMS only at the time the threshold is exceeded. (See [Figure 5](#) for a comparison of the warning and maximum thresholds.) Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS.

- **mplsNumVrfRouteMaxThreshExceeded**—Generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes as defined by the *limit* argument of the **maximum routes** commands:

```
Router(config)# ip vrf vrf-name
```

```
Router(config-vrf)# maximum routes limit warn-threshold (% of max)
```

A trap notification is sent to the NMS when you attempt to exceed the maximum threshold. Another **mplsNumVrfRouteMaxThreshExceeded** notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. (See [Figure 5](#) for an example of how this notification works and for a comparison of the maximum and warning thresholds.)

**Note**

The **maximum routes** command sets the number of routes for a VRF. You *cannot* exceed the number of routes in the VRF that you set with the **maximum routes** *limit warn-threshold* command.

Prior to this implementation of the PPVPN-MPLS-VPN MIB, you were not notified when this threshold (or the warning threshold) was reached.

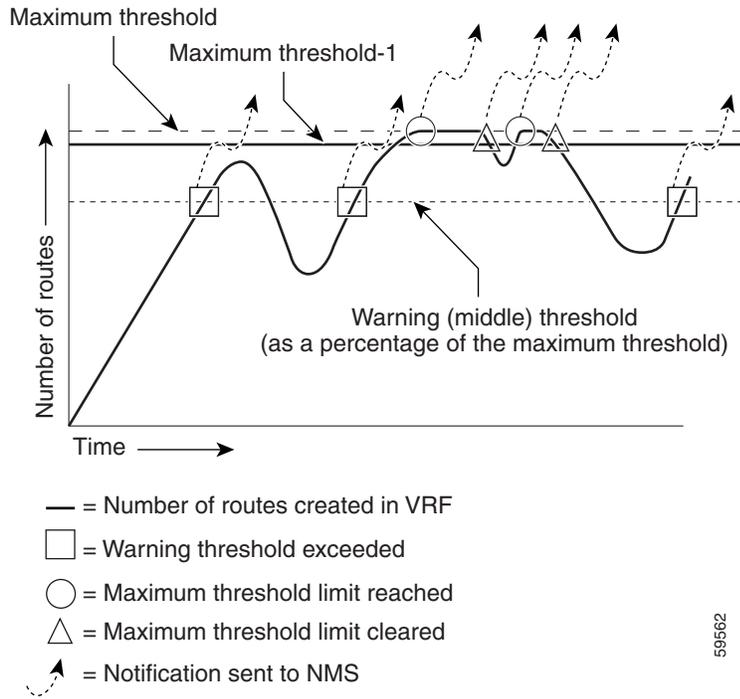
- **mplsNumVrfSecIllegalLabelThreshExceeded**—Generated and sent when the amount of illegal labels received on a VRF interface exceeds the threshold *mplsVpnVrfSecIllegalLabelRcvThresh*. This threshold is defined with a value of 0. Therefore, a notification is sent when the first illegal label is received on a VRF. Labels are considered illegal if they are outside of the valid label range, do not have a Label Forwarding Information Base (LFIB) entry, or the table ID of the message does not match the table ID for the label in the LFIB.

## CISCO-IETF-PPVPN-MPLS-VPN MIB Notification Events

The following notification of the CISCO-IETF-PPVPN-MPLS-VPN MIB is supported in Cisco IOS Release 12.0(30)S:

- **cMplsNumVrfRouteMaxThreshCleared**—Generated and sent when the number of routes on a VRF attempts to exceed the maximum number of routes and then drops below the maximum number of routes. **If you attempt to create a route on a VRF that already contains the maximum number of routes, the mplsNumVrfRouteMaxThreshExceeded notification is sent (if enabled). When you remove routes from the VRF so that the number of routes falls below the set limit, the cMplsNumVrfRouteMaxThreshCleared notification is sent.** You can clear all routes from the VRF by using the **clear ip route vrf** command. (See [Figure 5](#) to see when the **cMplsNumVrfRouteMaxThreshCleared** notification is sent.)

**Figure 5 Comparison of Warning and Maximum Thresholds**



59562

For information on the Cisco IOS CLI commands for configuring PPVPN-MPLS-VPN MIB notifications that are to be sent to an NMS, see the [“How to Configure PPVPN MPLS VPN MIB”](#) section on page 21 and the [“Feature Information for PPVPN MPLS VPN MIB”](#) section on page 31.

## Notification Specification

In an SNMPv1 notification, each VPN notification has a generic type identifier and an enterprise-specific type identifier for identifying the notification type.

- The generic type for all VPN notifications is “enterpriseSpecific” as this is not one of the generic notification types defined for SNMP.
- The enterprise-specific type is identified as follows:
  - 1 for *mplsVrfIfUp*
  - 2 for *mplsVrfIfDown*
  - 3 for *mplsNumVrfRouteMidThreshExceeded*
  - 4 for *mplsNumVrfRouteMaxThreshExceeded*
  - 5 for *mplsNumVrfSecIllegalLabelThreshExceeded*
  - 6 for *cMplsNumVrfRouteMaxThreshCleared*

In SNMPv2, the notification type is identified by an **SnmpTrapOID** varbind (variable binding consisting of an object identifier [OID] type and value) included within the notification message.

Each notification also contains two additional objects from the PPVPN-MPLS-VPN MIB. These objects provide additional information about the event, as follows:

- The VRF interface up/down notifications provide additional variables—*mplsVpnInterfaceConfIndex* and *mplsVpnVrfName*—in the notification. These variables describe the SNMP interface index and the VRF name, respectively.
- The mid and max threshold notifications include the *mplsVpnVrfName* variable (VRF name) as well as the *mplsVpnVrfPerfCurrNumRoutes* variable that indicates the current number of routes within the VRF.
- The illegal label notification includes the *mplsVpnVrfName* variable (VRF name) and the *mplsVpnVrfSecIllegalLabelViolations* variable that maintains the current count of illegal labels on a VPN.

## Monitoring the PPVPN-MPLS-VPN MIB Notifications

When PPVPN-MPLS-VPN MIB notifications are enabled (see the **snmp-server enable traps mpls vpn** command), notification messages relating to specific MPLS VPN events within Cisco IOS software are generated and sent to a specified NMS in the network. Any utility that supports SNMPv1 or SNMPv2 notifications can receive notification messages.

To monitor PPVPN-MPLS-VPN MIB notification messages, log in to an NMS that supports a utility that displays SNMP notifications, and start the display utility.

## MIB Objects Not Supported

The following objects from the *mplsVpnVrfBgpPathAttrTable* are not supported:

- *mplsVpnVrfBgpPathAttrPeer*
- *mplsVpnVrfBgpPathAttrIpAddrPrefixLen*
- *mplsVpnVrfBgpPathAttrIpAddrPrefix*
- *mplsVpnVrfBgpPathAttrOrigin*
- *mplsVpnVrfBgpPathAttrASPathSegment*

- `mplsVpnVrfBgpPathAttrNextHop`
- `mplsVpnVrfBgpPathAttrMultiExitDisc`
- `mplsVpnVrfBgpPathAttrLocalPref`
- `mplsVpnVrfBgpPathAttrAtomicAggregate`
- `mplsVpnVrfBgpPathAttrAggregatorAS`
- `mplsVpnVrfBgpPathAttrAggregatorAddr`
- `mplsVpnVrfBgpPathAttrCalcLocalPref`
- `mplsVpnVrfBgpPathAttrBest`
- `mplsVpnVrfBgpPathAttrUnknown`

## How to Configure PPVPN MPLS VPN MIB

This section describes configuration tasks for PPVPN MPLS VPN MIB. Each task in the list is identified as either required or optional.

- [Configuring the SNMP Community, page 21](#) (required)
- [Configuring the Router to Send SNMP Traps, page 23](#) (required)
- [Configuring Threshold Values for MPLS VPN—SNMP Notifications, page 25](#) (required)

### Configuring the SNMP Community

An SNMP community string defines the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the router.

Perform this task to configure an SNMP community.

#### SUMMARY STEPS

1. `enable`
2. `show running-config [options]`
3. `configure terminal`
4. `snmp-server community string [view view-name] [ro | rw] [acl-number]`
5. `do copy running-config startup-config`
6. `exit`
7. `show running-config [options]`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                  | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <p><b>show running-config</b> [<i>options</i>]</p> <p><b>Example:</b><br/>Router# show running-config</p>                                                                                                          | <p>Displays the running configuration to determine if an SNMP agent is already running.</p> <ul style="list-style-type: none"> <li>If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                             | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 4 | <p><b>snmp-server community</b> <i>string</i> [<b>view</b> <i>view-name</i>]<br/>[<b>ro</b>   <b>rw</b>] [<i>acl-number</i>]</p> <p><b>Example:</b><br/>Router(config)# snmp-server community comaccess<br/>ro</p> | <p>Sets up the community access string to permit access to the SNMP protocol.</p> <ul style="list-style-type: none"> <li>The <i>string</i> argument acts like a password and permits access to the SNMP protocol.</li> <li>The <b>view</b> <i>view-name</i> keyword argument pair specifies the name of a previously defined view. The view defines the objects available to the community.</li> <li>The <b>ro</b> keyword specifies read-only access. Authorized management stations are only able to retrieve MIB objects.</li> <li>The <b>rw</b> keyword specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.</li> <li>The <i>acl-number</i> argument is an integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.</li> </ul> |
| Step 5 | <p><b>do copy running-config startup-config</b></p> <p><b>Example:</b><br/>Router(config)# do copy running-config<br/>startup-config</p>                                                                           | <p>Saves the modified configuration to nonvolatile memory (NVRAM) as the startup configuration file.</p> <ul style="list-style-type: none"> <li>The <b>do</b> command allows you to perform EXEC level commands in configuration mode.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|        | Command or Action                                                    | Purpose                                                                                                                                                            |
|--------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>exit</b>                                                          | Returns to privileged EXEC mode.                                                                                                                                   |
|        | <b>Example:</b><br>Router(config)# exit                              |                                                                                                                                                                    |
| Step 7 | <b>show running-config</b> [ <i>options</i> ]                        | (Optional) Displays the configuration information currently on the router, the configuration for a specific interface, or map-class information.                   |
|        | <b>Example:</b><br>Router# show-running config   include snmp-server | <ul style="list-style-type: none"> <li>Use the <b>show running-config</b> command to check that the <b>snmp-server</b> statements appear in the output.</li> </ul> |

## Configuring the Router to Send SNMP Traps

Perform this task to configure the router to send traps to a host.

The **snmp-server host** command specifies which hosts receive traps. The **snmp-server enable traps** command globally enables the trap production mechanism for the specified traps.

For a host to receive a trap, an **snmp-server host** command must be configured for that host, and, generally, the trap must be enabled globally through the **snmp-server enable traps** command.



### Note

Although you can set the *community-string* argument using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command before using the **snmp-server host** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-addr* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]
4. **snmp-server enable traps mpls vpn** [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid-threshold**] [**vrf-down**] [**vrf-up**]
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                              | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <pre>configure terminal</pre> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                                                                                                                         | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <pre>snmp-server host host-addr [traps   informs] [version {1   2c   3 [auth   noauth   priv]]] community-string [udp-port port] [notification-type] [vrf vrf-name]</pre> <p><b>Example:</b><br/>Router(config)# snmp-server host 172.20.2.160 traps comaccess mpls-vpn</p> | <p>Specifies the recipient of an SNMP notification operation.</p> <ul style="list-style-type: none"> <li>• The <i>host-addr</i> argument specifies the name or Internet address of the host (the targeted recipient).</li> <li>• The <b>traps</b> keyword sends SNMP traps to this host. This is the default.</li> <li>• The <b>informs</b> keyword sends SNMP informs to this host.</li> <li>• The <b>version</b> keyword specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the <b>priv</b> keyword. If you use the <b>version</b> keyword, you must specify one of the following: <ul style="list-style-type: none"> <li>– <b>1</b> —SNMPv1. This option is not available with informs.</li> <li>– <b>2c</b> —SNMPv2C.</li> <li>– <b>3</b> —SNMPv3. The following three optional keywords can follow the <b>version 3</b> keyword (<b>auth</b>, <b>noauth</b>, <b>priv</b>).</li> </ul> </li> <li>• The <i>community-string</i> argument is a password-like community string sent with the notification operation.</li> <li>• The <b>udp-port port</b> keyword argument pair names the UDP port of the host to use. The default is 162.</li> <li>• The <i>notification-type</i> argument specifies the type of notification to be sent to the host. If no type is specified, all notifications are sent.</li> <li>• The <b>vrf vrf-name</b> keyword argument pair specifies the VRF table that should be used to send SNMP notifications.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <pre>snmp-server enable traps mpls vpn [illegal-label] [max-thresh-cleared] [max-threshold] [mid-threshold] [vrf-down] [vrf-up]</pre> <p><b>Example:</b><br/>Router(config)# snmp-server enable traps mpls<br/>vpn vrf-up vrf-down</p> | <p>Enables the router to send MPLS VPN specific SNMP notifications (traps and informs).</p> <ul style="list-style-type: none"> <li>• The <b>illegal-label</b> keyword enables a notification for any illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have an LFIB entry, or do not match table IDs for the label.</li> <li>• The <b>max-thresh-cleared</b> keyword enables a notification when the number of routes falls below the limit after the maximum route limit was attempted.</li> <li>• The <b>max-threshold</b> keyword enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached. Another <b>mplsNumVrfRouteMaxThreshExceeded</b> notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. The max-threshold value is determined by the <b>maximum routes</b> command in VRF configuration mode.</li> <li>• The <b>mid-threshold</b> keyword enables a notification of a warning that the number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded.</li> <li>• The <b>vrf-down</b> keyword enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.</li> <li>• The <b>vrf-up</b> keyword enables a notification for the assignment VRF to an interface that is operational or for the transition of a VRF interface to the operationally up state.</li> </ul> |
| Step 5 | <pre>end</pre> <p><b>Example:</b><br/>Router(config)# end</p>                                                                                                                                                                          | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Configuring Threshold Values for MPLS VPN—SNMP Notifications

Perform this task to configure the following threshold values for MPLS VPN—SNMP notifications:

- The **mplsNumVrfRouteMidThreshExceeded** notification event is generated and sent when the middle (warning) threshold is crossed. You can configure this threshold in the CLI by using the **maximum routes** command in VRF configuration mode. This notification is sent to the NMS only at the time the threshold is exceeded. Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS.
- The **mplsNumVrfRouteMaxThreshExceeded** notification event is generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes as defined by the **maximum routes** command in VRF configuration mode. A trap notification is sent to the

NMS when you attempt to exceed the maximum threshold. Another **mplsNumVrfRouteMaxThreshExceeded** notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again.

See [Figure 5](#) for an example of how this notification works and for a comparison of the maximum and warning thresholds.



**Note** The **maximum routes** command sets the number of routes for a VRF. You *cannot* exceed the number of routes in the VRF that you set with the **maximum routes limit warn-threshold** command.

Prior to this implementation of the PPVPN-MPLS-VPN MIB, you were not notified when this threshold (or the warning threshold) was reached.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **maximum routes limit** {*warn-threshold* | **warn-only**}
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                   | Purpose                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal      | Enters global configuration mode.                                                                                                                                                        |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# ip vrf vpn1 | Configures a VRF routing table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>• The <i>vrf-name</i> argument specifies the name assigned to a VRF.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <pre>maximum routes limit {warn-threshold   warn-only}</pre> <p><b>Example:</b><br/>Router(config-vrf)# maximum routes 10000 80<br/>or</p> <p><b>Example:</b><br/>Router(config-vrf)# maximum routes 10000 warn-only</p> | <p>Limits the maximum number of routes in a VRF to prevent a PE router from importing too many routes.</p> <ul style="list-style-type: none"> <li>The <i>limit</i> argument specifies the maximum number of routes allowed in a VRF. The range is from 1 to 4,294,967,295.</li> <li>The <i>warn-threshold</i> argument generates a warning when the number of routes set by the <i>warn-threshold</i> argument is reached and rejects routes that exceed the maximum number set in the <i>limit</i> argument. The warning threshold is a percentage from 1 to 100 of the maximum number of routes specified in the <i>limit</i> argument.</li> <li>The <b>warn-only</b> keyword specifies that a SYSLOG error message is issued when the maximum number of routes allowed for a VRF exceeds the limit threshold. However, additional routes are still allowed.</li> </ul> |
| Step 5 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-vrf)# end</p>                                                                                                                                                        | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Configuration Examples for PPVPN MPLS VPN MIB

This section contains the following configuration examples for the PPVPN MPLS VPN MIB feature:

- [Configuring the SNMP Community: Examples, page 27](#)
- [Configuring the Router to Send SNMP Traps: Example, page 28](#)
- [Configuring Threshold Values for MPLS VPN—SNMP Notifications: Examples, page 28](#)

### Configuring the SNMP Community: Examples

The following example shows enabling a simple SNMP community group. This configuration permits any SNMP client to access all PPVPN-MPLS-VPN MIB objects with read-only access using the community string comaccess.

```
Router# configure terminal
```

```
Router(config)# snmp-server community comaccess ro
```

Verify that the SNMP master agent is enabled for the PPVPN MPLS VPN MIB feature:

```
Router# show running-config | include snmp-server

Building configuration...
....
snmp-server community comaccess RO
....
```


**Note**

If you do not see any “snmp-server” statements, SNMP is not enabled on the router.

## Configuring the Router to Send SNMP Traps: Example

The following example shows you how to enable the router to send MPLS VPN notifications to host 172.20.2.160 using the comaccess community string if a VRF transitions from an up or down state.

```
Router# configure terminal

Router(config)# snmp-server host 172.20.2.160 traps comaccess mpls-vpn

Router(config)# snmp-server enable traps mpls vpn vrf-up vrf-down
```

## Configuring Threshold Values for MPLS VPN—SNMP Notifications: Examples

The following example shows how to set a maximum threshold of 10000 routes and a warning threshold that is 80 percent of the maximum threshold for a VRF named vpn1 on a router:

```
Router(config)# ip vrf vpn1

Router(config-vrf)# maximum routes 10000 80
```

The following example shows how to set a warning threshold of 10000 routes for a VRF named vpn2 on a router. An error message is generated; however, additional routes are still allowed because a maximum route threshold is not set with this command.

```
Router(config)# ip vrf vpn2

Router(config-vrf)# maximum routes 10000 warn-only
```

# Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic MPLS VPNs                     | <a href="#">Configuring MPLS Layer 3 VPNs</a><br><a href="#">Configuring Scalable Hub-and-Spoke MPLS VPNs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li>• <a href="#">Enabling One Carrier to Supply MPLS Services to Another Carrier Through MPLS VPN Carrier Supporting Carrier with BGP</a></li> <li>• <a href="#">Preserving QoS Settings in an MPLS VPN Carrier Supporting Carrier Network</a></li> <li>• <a href="#">Using MPLS Static Labels at the Edge of the MPLS VPN Carrier Supporting Carrier Network</a></li> </ul> |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> <li>• <a href="#">Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> </ul>                                                                                                                                                                                                          |
| MPLS VPN route maps                 | <a href="#">Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MPLS VPN load sharing               | <a href="#">Load Sharing MPLS VPN Traffic</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Directing MPLS VPN traffic          | <ul style="list-style-type: none"> <li>• <a href="#">Directing MPLS VPN Traffic Using Policy-Based Routing</a></li> <li>• <a href="#">Directing MPLS VPN Traffic Using a Source IP Address</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| VPN ID                              | <a href="#">Assigning an ID Number to a VPN</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Dialer applications with MPLS VPNs  | <ul style="list-style-type: none"> <li>• <a href="#">Dialing to Destinations with the Same IP Address for MPLS VPNs</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MPLS VPNs and OSPF                  | <a href="#">Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links</a>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Standards

| Standard                                         | Title                                                                                     |
|--------------------------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">draft-ietf-ppvpn-mpls-vpn-mib-03</a> | <a href="#">MPLS/BGP Virtual Private Network Management Information Base Using SMIPv2</a> |

## MIBs

| MIB                                                                                                   | MIBs Link                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>MPLS-VPN-MIB</li> <li>CISCO-IETF-PPVPN-MPLS-VPN-MIB</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC         | Title                                        |
|-------------|----------------------------------------------|
| RFC 2233    | <i>The Interfaces Group MIB using SMIPv2</i> |
| RFC 2547bis | <i>BGP/MPLS VPNs</i>                         |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for PPVPN MPLS VPN MIB

Table 9 lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “[MPLS Layer 3 VPN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 9 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 9** Feature Information for Monitoring MPLS VPNs with MIBs

| Feature Name         | Releases                                                                                  | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—MIB Support | 12.0(21)ST<br>12.0(22)S<br>12.2(13)S<br>12.2(15)T<br>12.0(24)S1<br>12.0(25)S<br>12.0(30)S | <p>This feature allows you to monitor and manage MPLS VPNs using MIBs.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">MPLS VPN Overview, page 2</a></li> <li><a href="#">PPVPN MPLS VPN MIB Overview, page 3</a></li> <li><a href="#">PPVPN MPLS VPN MIB and the IETF, page 3</a></li> <li><a href="#">Capabilities Supported by PPVPN-MPLS-VPN MIB, page 4</a></li> <li><a href="#">Functional Structure of the PPVPN-MPLS-VPN MIB, page 4</a></li> <li><a href="#">Supported Objects in PPVPN-MPLS-VPN MIB, page 4</a></li> <li><a href="#">MIB Objects Not Supported, page 20</a></li> <li><a href="#">How to Configure PPVPN MPLS VPN MIB, page 21</a></li> </ul> |

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.