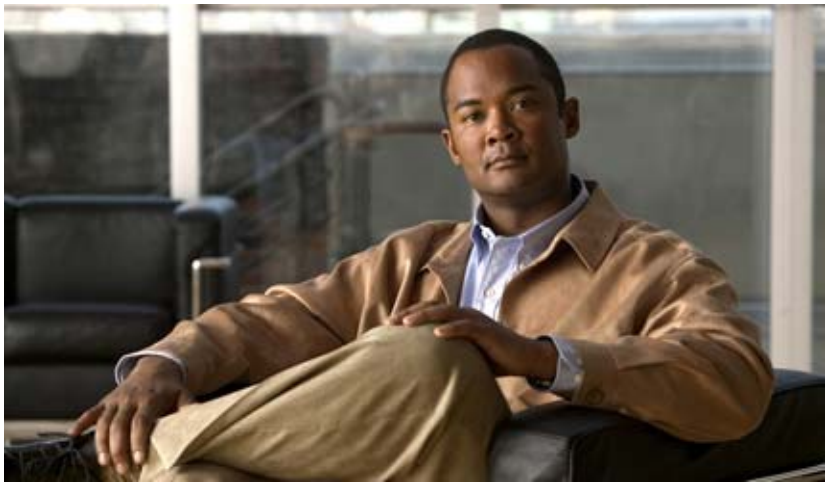


Cisco IOS Multiprotocol Label Switching Command Reference

January 2010

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.

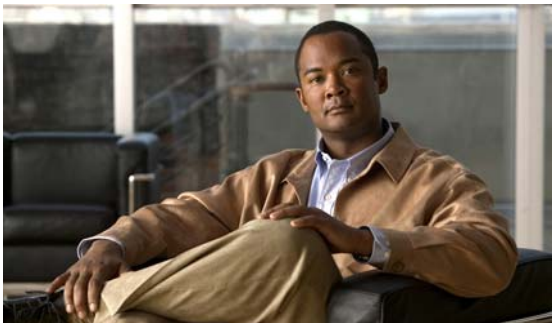
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

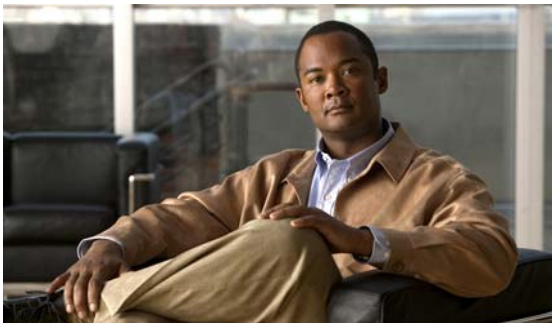
All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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 Command Reference
© 2000—2010 Cisco Systems, Inc. All rights reserved.



CONTENTS



About Cisco IOS Software Documentation

Last Updated: November 20, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software 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

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 software 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 contains the following topics:

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.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, 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.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets 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 software 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.
`Bold 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

Cisco IOS documentation 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. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

Cisco IOS Documentation Set

The Cisco IOS documentation set 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 select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether 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 conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports 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 organization of the Cisco IOS documentation set 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 contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized 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/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xxvii.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references contain commands for Cisco IOS 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.

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.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

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

Table 1 Cisco IOS Configuration Guides and Command References

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

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging Command Reference* • *Cisco IOS IBM Networking Command Reference*	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.
• *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).
• *Cisco IOS Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	Operations, Administration, and Maintenance (OAM); Ethernet connectivity fault management (CFM); ITU-T Y.1731 fault management functions; Ethernet Local Management Interface (ELMI); MAC address support on service instances, bridge domains, and pseudowire; IEEE 802.3ad Link Bundling; Link Aggregation Control Protocol (LACP) support for Ethernet and Gigabit Ethernet links and EtherChannel bundles; LACP support for stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles; and Link Layer Discovery Protocol (LLDP) and media endpoint discovery (MED).
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	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.
• *Cisco IOS DECnet Configuration Guide* • *Cisco IOS DECnet Command Reference*	DECnet protocol.
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS Flexible NetFlow Configuration Guide* • *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS High Availability Configuration Guide* • *Cisco IOS High Availability Command Reference*	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.
• *Cisco IOS Integrated Session Border Controller Command Reference*	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).
• *Cisco IOS Intelligent Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
• *Cisco IOS Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
• *Cisco IOS IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
• *Cisco IOS IP Application Services Configuration Guide* • *Cisco IOS IP Application Services Command Reference*	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).
• *Cisco IOS IP Mobility Configuration Guide* • *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
• *Cisco IOS IP Multicast Configuration Guide* • *Cisco IOS IP Multicast Command Reference*	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).
• *Cisco IOS IP Routing: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).
• *Cisco IOS IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
• *Cisco IOS IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	Routing Information Protocol (RIP).
• *Cisco IOS IP SLAs Configuration Guide* • *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
• *Cisco IOS IP Switching Configuration Guide* • *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
• *Cisco IOS IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document.
• *Cisco IOS ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).
• *Cisco IOS LAN Switching Configuration Guide* • *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
• *Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide* • *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	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.
• *Cisco IOS Mobile Wireless Home Agent Configuration Guide* • *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
• *Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide* • *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	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.
• *Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide* • *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Multiprotocol Label Switching Configuration Guide* • *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.
• *Cisco IOS Multi-Topology Routing Configuration Guide* • *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
• *Cisco IOS NetFlow Configuration Guide* • *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, and export features.
• *Cisco IOS Network Management Configuration Guide* • *Cisco IOS Network Management Command Reference*	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).
• *Cisco IOS Novell IPX Configuration Guide* • *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
• *Cisco IOS Optimized Edge Routing Configuration Guide* • *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
• *Cisco IOS Security Command Reference*	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.
• *Cisco IOS Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS Security Configuration Guide: Securing the Control Plane*	Control Plane Policing, Neighborhood Router Authentication.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Security Configuration Guide: Securing User Services*	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
• *Cisco IOS Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.
• *Cisco IOS Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *Cisco IOS Service Selection Gateway Configuration Guide* • *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
• *Cisco IOS Software Activation Configuration Guide* • *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
• *Cisco IOS Software Modularity Installation and Configuration Guide* • *Cisco IOS Software Modularity Command Reference*	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.
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
• *Cisco IOS Virtual Switch Command Reference*	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, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
• *Cisco IOS VPDN Configuration Guide* • *Cisco IOS VPDN Command Reference*	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.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
• *Cisco IOS Wireless LAN Configuration Guide* • *Cisco IOS Wireless LAN Command Reference*	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 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS System Message Guide	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software.
Cisco IOS Debug Command Reference	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.
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 released 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

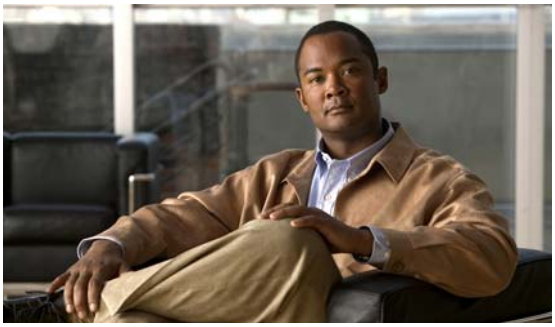
Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface in Cisco IOS Software

Last Updated: October 14, 2009

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

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 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/Technologies Support area of Cisco.com at http://www.cisco.com/go/techdocs.

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 ASR 1000 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

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 3 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 3 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• 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.	• 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 3 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.	• 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 Cisco ASR 1000 series routers)	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. • 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)#`	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. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI. 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.	• 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 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 4 describes the purpose of the CLI interactive Help commands.

Table 4 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.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	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 5 describes these conventions.

Table 5 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
```

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 numeral. 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 numeral 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 command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands 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 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 **vrrp** as a keyword in addition to **version**. (Command and keyword examples are 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 6 shows the default command aliases.

Table 6 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_a1.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** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

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 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.

The following three output modifiers are available:

- **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 7 shows the common CLI error messages.

Table 7 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 document:

- *Cisco IOS Release 12.4T System Message Guide*

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
- Cisco Product/Technology Support

  http://www.cisco.com/go/techdocs
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- 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/pcgi-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

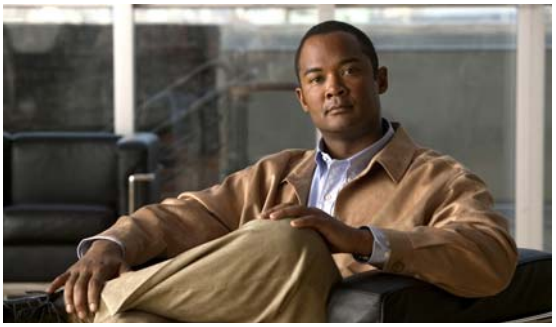
---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Multiprotocol Label Switching Commands

address-family

To enter the address family submode for configuring routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and static routing, use the **address-family** command in address family configuration submode. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

VPN-IPv4 Unicast

address-family vpnv4 [**unicast**]

no address-family vpnv4 [**unicast**]

IPv4 Unicast

address-family ipv4 [**unicast**]

no address-family ipv4 [**unicast**]

IPv4 Unicast with CE router

address-family ipv4 [**unicast**] **vrf** *vrf-name*

no address-family ipv4 [**unicast**] **vrf** *vrf-name*

Syntax Description

vpnv4	Configures sessions that carry customer Virtual Private Network (VPN)-IPv4 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher.
ipv4	Configures sessions that carry standard IPv4 address prefixes.
unicast	(Optional) Specifies unicast prefixes.
vrf *vrf-name*	Specifies the name of a VPN routing/forwarding instance (VRF) to associate with submode commands.

Defaults

Routing information for address family IPv4 is advertised by default when you configure a BGP session using the **neighbor remote-as** command unless you execute the **no bgp default ipv4-activate** command.

Command Modes

Address family configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **address-family** command puts the router in address family configuration submode (prompt: `(config-router-af)#`). Within this submode, you can configure address-family specific parameters for routing protocols, such as BGP, that can accommodate multiple Layer 3 address families.

To leave address family configuration submode and return to router configuration mode, enter the **exit-address-family** or **exit** command.

Examples

The **address-family** command in the following example puts the router into address family configuration submode for the VPNv4 address family. Within the submode, you can configure advertisement of Network Layer Reachability Information (NLRI) for the VPNv4 address family using **neighbor activate** and other related commands:

```
router bgp 100
address-family vpnv4
```

The **address-family** command in the following example puts the router into address family configuration submode for the IPv4 address family. Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices. This **address-family** command causes subsequent commands entered in the submode to be executed in the context of VRF vrf2. Within the submode, you can use **neighbor activate** and other related commands to accomplish the following:

- Configure advertisement of IPv4 NLRI between the PE and CE routers.
- Configure translation of the IPv4 NLRI (that is, translate IPv4 into VPNv4 for NLRI received from the CE, and translate VPNv4 into IPv4 for NLRI to be sent from the PE to the CE).
- Enter the routing parameters that apply to this VRF.

The following example shows how to enter the address family submode:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 unicast vrf vrf2
```

Related Commands

Command	Description
default	Exits from address family submode.
neighbor activate	Enables the exchange of information with a neighboring router.

affinity (LSP Attributes)

To specify attribute flags for links of a label switched path (LSP) in an LSP attribute list, use the **affinity** command in LSP Attributes configuration mode. To remove the specified attribute flags, use the **no** form of this command.

affinity *value* [**mask** *value*]

no affinity

Syntax Description

value	Attribute flag value required for links that make up an LSP. Values of the bits are either 0 or 1.
mask *value*	(Optional) Indicates which attribute values should be checked. If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.

Command Default

Attribute values are not checked.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set the affinity and affinity mask values for an LSP in an LSP attribute list.

The affinity value determines the attribute flags for links that make up the LSP, either 0 or 1. The attribute mask determines which attribute value the router should check. If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of a link and the required affinity of the LSP for that bit must match.

An LSP can use a link if the link affinity equals the attribute flag value and the affinity mask value.

Any value set to 1 in the affinity should also be set to 1 in the mask.

To associate the LSP affinity attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example sets the affinity values for a path option in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes 1
 affinity 0 mask 0
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

allocate

To configure local label allocation filters for learned routes for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), use the **allocate** command in MPLS LDP label configuration mode. To remove the specific MPLS LDP local label allocation filter without resetting the LDP session, use the **no** form of this command.

allocate global {**prefix-list** {*list-name* | *list-number*} | **host-routes**}

no allocate global {**prefix-list** {*list-name* | *list-number*} | **host-routes**}

Syntax Description

global	Specifies the global routing table.
prefix-list	Specifies a prefix list to be used as a filter for MPLS LDP local label allocation.
list-name	Name that identifies the prefix list.
list-number	Number that identifies the prefix list.
host-routes	Specifies that host routes be used as a filter for MPLS LDP local label allocation.

Command Default

Prefix filters are not configured for MPLS LDP local label allocation.

Command Modes

MPLS LDP label configuration (config-ldp-lbl)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

LDP allocates local labels for all learned routes or prefixes. Use the **allocate** command to specify a prefix list or a host route to control local label allocation filtering.

If you configure the **allocate** command with a prefix list as the filter and the prefix list does not exist, a prefix list is created that initially permits all prefixes.

You can configure only one prefix list for the global routing table. Configuring a different prefix list overrides the existing configuration.

If you configure the **allocate** command with host routes as the filter, then LDP allocates local labels for host routes only.

The **no** form in a specific **allocate** command removes that particular local label allocation configuration from the global table.

Examples

The following example shows how to configure a prefix list named List1 found in the global routing table as a filter for MPLS LDP local label allocation:

```
configure terminal
!
mpls ldp label
 allocate global prefix-list List1
 end
```

LDP allocates local labels only for prefixes that match the configured prefix list.

The following example shows how to remove a local label allocation filter:

```
configure terminal
!
mpls ldp label
 no allocate global prefix-list List1
 end
```

The following example shows how to configure host routes as the filter for the MPLS LDP local label allocation:

```
configure terminal
!
mpls ldp label
 allocate global host-routes
 end
```

LDP allocates local labels only for host routes found in the global routing table.

Related Commands

Command	Description
mpls ldp label	Enters MPLS LDP label configuration mode to specify how MPLS LDP handles local label allocation.
show mpls ldp bindings	Displays the contents of the LIB.

append-after

To insert a path entry after a specified index number, use the **append-after** command in IP explicit path configuration mode.

append-after *index command*

Syntax Description

index	Previous index number. Valid values are from 0 to 65534.
command	An IP explicit path configuration command that creates a path entry. (Use the **next-address** command to specify the next IP address in the explicit path.)

Defaults

No path entry is inserted after a specified index number.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the **next-address** command is inserted after index 5:

```
Router(config-ip-expl-path)# append-after 5 next-address 10.3.27.3
```

Related Commands

Command	Description
index	Inserts or modifies a path entry at a specific index.
interface fastethernet	Enters the command mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

auto-bw (LSP Attributes)

To specify automatic bandwidth configuration for a label switched path (LSP) in an LSP attribute list, use the **auto-bw** command in LSP Attributes configuration mode. To remove automatic bandwidth configuration, use the **no** form of this command.

auto-bw [**frequency** *secs*] [**max-bw** *kbps*] [**min-bw** *kbps*] [**collect-bw**]

no auto-bw

Syntax Description

frequency *secs*	(Optional) Interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds.
max-bw *kbps*	(Optional) Maximum automatic bandwidth for the path option. The value can be from 0 to 4294967295 kilobits per second (kbps).
min-bw *kbps*	(Optional) Minimum automatic bandwidth for the path option. The value is from 0 to 4294967295 kilobits per second (kbps).
collect-bw	(Optional) Collects output rate information for the path option, but does not adjust its bandwidth.

Command Default

If the command is entered with no optional keywords, automatic bandwidth adjustment for the LSP is enabled, with adjustments made every 24 hours and with no constraints on the bandwidth adjustments made.
If the **collect-bw** keyword is entered, the bandwidth is sampled but not adjusted, and the other options, if any, are ignored.
If the **collect-bw** keyword is not entered and some, but not all of the other keywords are entered, the defaults for the keywords not entered are: **frequency**, every 24 hours; **min-bw**, unconstrained (0); **max-bw**, unconstrained.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set an automatic bandwidth configuration in an LSP attributes list.

To sample the bandwidth used by an LSP without automatically adjusting it, specify the **collect-bw** keyword in the **auto-bw** command in an LSP attribute list.

If you enter the **auto-bw** command without the **collect-bw** keyword, the bandwidth of the LSP is adjusted to the largest average output rate sampled for the LSP since the last bandwidth adjustment for the LSP was made.

To constrain the bandwidth adjustment that can be made to an LSP in an LSP attribute list, use the **max-bw** or **min-bw** keyword and specify the permitted maximum allowable bandwidth or minimum allowable bandwidth, respectively.

The **no** form of the **auto-bw** command disables bandwidth adjustment for the tunnel and restores the configured bandwidth for the LSP where configured bandwidth is determined as follows:

- If the LSP bandwidth was explicitly configured with the **mpls traffic-eng lsp attributes lsp-id 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.

To associate the LSP automatic bandwidth adjustment attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example sets automatic bandwidth configuration for an LSP in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes 1
 auto-bw
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

bandwidth (LSP Attributes)

To configure label switched path (LSP) bandwidth in an LSP attribute list, use the **bandwidth** command in LSP Attributes configuration mode. To remove the configured bandwidth from the LSP attribute list, use the **no** form of this command.

bandwidth [**sub-pool** | **global**] *kbps*

no bandwidth

Syntax Description

sub-pool	(Optional) Indicates a subpool path option.
global	(Optional) Indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.
kbps	Number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.

Command Default

The default bandwidth is 0.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure LSP bandwidth in the LSP attribute list. The bandwidth configured can be associated with both dynamic and explicit path options.

To associate the LSP bandwidth and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

The bandwidth configured in the LSP attribute list will override the bandwidth configured on the tunnel.

Examples

The following example shows how to set the LSP bandwidth to 5000 kbps in the LSP attribute list identified with the numeral 2:

```
configure terminal
!
mpls traffic-eng lsp attributes 2
 bandwidth 5000
```

```
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

bgp default route-target filter

To enable automatic Border Gateway Protocol (BGP) default route-target community filtering, use the **bgp default route-target filter** command in router configuration mode. To disable automatic BGP route-target community filtering, use the **no** form of this command.

bgp default route-target filter

no bgp default route-target filter

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(16)ST	This command was integrated into Cisco IOS Release 12.0(16)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **bgp default route-target filter** command to control the distribution of Virtual Private Network (VPN) routing information through the list of VPN route-target communities.

When you use the **no** form of this command, all received VPN-IPv4 routes are accepted by the configured router. Accepting VPN-IPv4 routes is the desired behavior for a router configured as an autonomous system border edge router or as a customer edge (CE) BGP border edge router.

If you configure the router for BGP route-target community filtering, all received exterior BGP (eBGP) VPN-IPv4 routes are discarded when those routes do not contain a route-target community value that matches the import list of any configured VPN routing and forwarding (VRFs) instances. This is the desired behavior for a router configured as a provider edge (PE) router.

Note This command is automatically disabled if a PE router is configured as a client of a common VPN-IPv4 route reflector in the autonomous system.

Examples

In the following example, BGP route-target filtering is disabled for autonomous system 120:

```
router bgp 120
 no bgp default route-target filter
```

Related Commands

Command	Description
show mpls forwarding-table	Displays the contents of the LFIB.

bgp next-hop

To configure a loopback interface as the next hop for routes associated with a VPN routing and forwarding instance (VRF), use the **bgp next-hop** command in VRF configuration mode. To return the router to default operation, use the **no** form of this command.

bgp next-hop loopback *number*

no bgp next-hop

Syntax Description

loopback *number*	Specifies the number of the loopback interface. The value that can be entered for this argument is a number from 1 to 2147483647.

Defaults

The IP address of the source interface, from which the route was advertised is set as the next hop when this command is not enabled.

Command Modes

VRF configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **bgp next-hop** command is used in Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) and Tunnel Engineering (TE) configurations. This command allows you to configure a loopback interface as the next hop for routes that are associated with the specified VRF. This command can be used, for example, to configure VPN traffic to use a specific Label Switched Path (LSP) through an MPLS core network.

Examples

In the following example, loopback interface 0 is configured as the next hop for VPN traffic associated with VRF RED:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 40000:1
Router(config-vrf)# route-target import 40000:2
Router(config-vrf)# route-target export 40000:2
Router(config-vrf)# bgp next-hop loopback 0
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP) routers for next hop validation or to decrease import processing time of Virtual Private Network version 4 (VPNv4) routing information, use the **bgp scan-time** command in address family or router configuration mode. To return the scanning interval of a router to its default scanning interval of 60 seconds, use the **no** form of this command.

bgp scan-time [**import**] *scanner-interval*

no bgp scan-time [**import**] *scanner-interval*

Syntax Description

import	(Optional) Configures import processing of VPNv4 unicast routing information from BGP routers into routing tables.
scanner-interval	The scanning interval of BGP routing information. Valid values used for selecting the desired scanning interval are from 5 to 60 seconds. The default is 60 seconds.

Command Default

The default scanning interval is 60 seconds.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. The **import** keyword was removed. It is not available in Cisco IOS Release 15.0(1)M and later Cisco IOS Release 15.0M releases.
12.2(33)SRE	This command was modified. The **import** keyword was removed. It is not available in Cisco IOS Release 12.2(33)SRE and later Cisco IOS Release 12.2SR releases.

Usage Guidelines

Entering the **no** form of this command does not disable scanning, but removes it from the output of the **show running-config** command.

The **import** keyword is supported in address family VPNv4 unicast mode only.

The BGP Event Based VPN Import feature introduced a modification to the existing BGP path import process using new commands and the **import** keyword was removed from the **bgp scan-time** command in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases.

Examples

In the following router configuration example, the scanning interval for next hop validation of IPv4 unicast routes for BGP routing tables is set to 20 seconds:

```
router bgp 100
 no synchronization
 bgp scan-time 20
```

In the following address family configuration example, the scanning interval for next hop validation of address family VPNv4 unicast routes for BGP routing tables is set to 45 seconds:

```
router bgp 150
 address-family vpn4 unicast
  bgp scan-time 45
```

In the following address family configuration example, the scanning interval for importing address family VPNv4 routes into IP routing tables is set to 30 seconds:

```
router bgp 150
 address-family vpnv4 unicast
  bgp scan-time import 30
```

Related Commands

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

cell-packing

To enable ATM over Multiprotocol Label Switching (MPLS) or Layer 2 Tunneling Protocol Version 3 (L2TPv3) to pack multiple ATM cells into each MPLS or L2TPv3 packet, use the **cell-packing** command in the appropriate configuration mode. To disable cell packing, use the **no** form of this command.

cell-packing [*cells*] [**mcpt-timer** *timer*]

no cell-packing

Syntax Description

cells	(Optional) The number of cells to be packed into an MPLS or L2TPv3 packet. The range is from 2 to the maximum transmission unit (MTU) of the interface divided by 52. The default number of ATM cells to be packed is the MTU of the interface divided by 52. If the number of cells packed by the peer provider edge router exceeds this limit, the packet is dropped.
mcpt-timer *timer*	(Optional) Specifies which timer to use for maximum cell-packing timeout (MCPT). Valid values are **1**, **2**, or **3**. The default value is **1**.

Command Default

Cell packing is disabled.

Command Modes

Interface configuration
L2transport VC configuration—for ATM VC
L2transport VP configuration—for ATM VP
VC class configuration

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.0(29)S	Support for L2TPv3 sessions was added.
12.0(30)S	This command was updated to enable cell packing as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was modified. Support for static pseudowires was added.

Usage Guidelines

The **cell-packing** command is available only if you configure the ATM VC or virtual path (VP) with ATM adaptation layer 0 (AAL0) encapsulation. If you specify ATM adaptation layer 5 (AAL5) encapsulation, the command is not valid.

Only cells from the same VC or VP can be packed into one MPLS or L2TPv3 packet. Cells from different connections cannot be concatenated into the same packet.

When you change, enable, or disable the cell-packing attributes, the ATM VC or VP and the MPLS or L2TPv3 emulated VC are reestablished.

If a provider edge (PE) router does not support cell packing, the PE router sends only one cell per MPLS or L2TPv3 packet.

The number of packed cells need not 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 or L2TPv3 packet and PE2 is allowed to pack 20 cells per MPLS or L2TPv3 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 packet is dropped.

If you issue the **cell-packing** command without first specifying the **atm mcpt-timers** command, you get the following error:

```
Please set mcpt values first
```

In order to support cell packing for static pseudowires, both PEs must run Cisco IOS Release 12.2(1)SRE, and the maximum number of cells that can be packed must be set to the same value on each.

Examples

The following example shows cell packing enabled on an interface set up for VP mode. The **cell-packing** command specifies that ten ATM cells be packed into each MPLS packet. The command also specifies that the second maximum cell-packing timeout (MCPT) timer be used.

```
Router> enable
Router# configure terminal
Router(config)# interface atm1/0
Router(config-if)# atm mcpt-timers 1000 800 500
Router(config-if)# atm pvp 100 l2transport
Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 234 encapsulation mpls
Router(config-if-atm-l2trans-pvp)# cell-packing 10 mcpt-timer 2
```

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.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm cellpacking
Router(config-vc-class)# encapsulation aal0
Router(config-vc-class)# cell-packing 10 mcpt-timer 1
Router(config-vc-class)# exit
Router(config)# interface atm1/0
Router(config-if)# atm mcpt-timers 100 200 250
Router(config-if)# class-int cellpacking
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures ATM AAL5 over L2TPv3 in VC class configuration mode. The VC class is then applied to an interface.

```
Router(config)# vc-class atm aal5class
Router(config-vc-class)# encapsulation aal5
!
Router(config)# interface atm1/0
Router(config-if)# class-int aal5class
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation l2tpv3
```

Related Commands

Command	Description
atm mcpt-timers	Creates cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS or L2TPv3 packet.
debug atm cell-packing	Displays ATM cell relay cell packing debugging information.
show atm cell-packing	Displays information about the VCs and VPs that have ATM cell packing enabled.

class (MPLS)

To configure a defined Multiprotocol Label Switching (MPLS) class of service (CoS) map that specifies how classes map to label switched controlled virtual circuits (LVCs) when combined with a prefix map, use the **class** command in CoS map submode. To remove the defined MPLS CoS map, use the **no** form of this command.

class *class* [**available** | **standard** | **premium** | **control**]

no class *class* [**available** | **standard** | **premium** | **control**]

Syntax Description

class	The precedence of identified traffic to classify traffic.
available	(Optional) Means low precedence (In/Out plus lower two bits = 0,4).
standard	(Optional) Means next precedence (In/Out plus lower two bits = 1,5).
premium	(Optional) Means high precedence (In/Out plus lower two bits = 2,6).
control	(Optional) Means highest precedence pair (In/Out plus lower two bits = 3,7). These bits are reserved for control traffic.

Defaults

This command is disabled.

Command Modes

CoS map submode

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure a CoS map:

```
Router(config)# mpls cos-map 55
Router(config-mpls-cos-map)# class 1 premium
Router(config-mpls-cos-map)# exit
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
mpls cos-map	Creates a class map that specifies how classes map to LVCs when combined with a prefix map.

Command	Description
mpls prefix-map	Configures a router to use a specified quality of service (QoS) map when a label definition prefix matches the specified access list.
show mpls cos-map	Displays the CoS map used to assign quantity of LVCs and associated CoS of those LVCs.

clear ip route vrf

To remove routes from the Virtual Private Network (VPN) routing and forwarding(VRF) table, use the **clear ip route vrf** command in user EXEC or privileged EXEC mode.

clear ip route vrf *vrf-name* {***** | *network* [*mask*]}

Syntax Description

vrf-name	Name of the VRF for the static route.
*****	Indicates all routes for a given VRF.
network	Destination to be removed, in dotted decimal format.
mask	(Optional) Mask for the specified network destination, in dotted decimal format.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to clear routes from the routing table. Use the asterisk (*) to delete all routes from the forwarding table for a specified VRF, or enter the address and mask of a particular network to delete the route to that network.

Examples

The following command shows how to remove the route to the network 10.13.0.0 in the vpn1 routing table:

```
Router# clear ip route vrf vpn1 10.13.0.0
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.

clear ip rsvp hello bfd

To globally reset to zero the number of times that the Bidirectional Forwarding Detection (BFD) protocol was dropped on an interface or the number of times that a link was down, use the **clear ip rsvp hello bfd** command in user EXEC or privileged EXEC mode. To disable the resetting of those counters, use the **no** form of this command.

clear ip rsvp hello bfd {**lost-cnt** | **nbr-lost**}

no clear ip rsvp hello bfd {**lost-cnt** | **nbr-lost**}

Syntax Description

lost-cnt	Resets to zero the number of times that the BFD session was lost (dropped) on an interface.
nbr-lost	Resets to zero the number of times the BFD protocol detected that a link was down.

Command Default

The counters are not reset to zero.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

When you unconfigure BFD-triggered Fast Reroute, the BFD session is not torn down. Enter the **clear ip rsvp hello bfd** command to clear **show** command output for Multiprotocol Label Switching (MPLS) traffic engineering (TE) features that use the BFD protocol.

The **clear ip rsvp hello bfd** command globally resets to zero the LostCnt field in the **show ip rsvp hello bfd nbr summary** command and the **show ip rsvp hello bfd nbr** command. Those fields show the number of times that the BFD session was lost (dropped) on an interface.

The **clear ip rsvp hello bfd** command also resets to zero the Communication with neighbor lost field in the **show ip rsvp hello bfd nbr detail** command. That field shows the number of times the BFD protocol detected that a link was down.

Examples

The following example resets to zero the Communication with neighbor lost field in the **show ip rsvp hello bfd nbr detail** command that shows the number of times the BFD protocol detected that a link was down:

```
Router# clear ip rsvp hello bfd nbr-lost
```

Related Commands

Command	Description
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

clear ip rsvp hello instance counters

To clear (refresh) the values for Hello instance counters, use the **clear ip rsvp hello instance counters** command in privileged EXEC mode.

clear ip rsvp hello instance counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.

Examples

Following is sample output from the **show ip rsvp hello instance detail** command and then the **clear ip rsvp hello instance counters** command. Notice that the "Statistics" fields have been cleared to zero.

```
Router# show ip rsvp hello instance detail

Neighbor 10.0.0.2  Source  10.0.0.1
    State: UP      (for 2d18h)
    Type: PASSIVE  (responding to requests)
    I/F: Et1/1
    LSPs protecting: 0
    Refresh Interval (msec) (used when ACTIVE)
      Configured: 100
      Statistics: (from 2398195 samples)
        Min:      100
        Max:      132
        Average:  100
        Waverage: 100 (Weight = 0.8)
        Current:  100
```

```
    Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
    Counters:
      Communication with neighbor lost:
        Num times: 0
        Reasons:
          Missed acks:             0
          Bad Src_Inst received:   0
          Bad Dst_Inst received:   0
          I/F went down:           0
          Neighbor disabled Hello: 0
      Msgs Received:   2398194
           Sent:       2398195
           Suppressed: 0

Router# clear ip rsvp hello instance counters

Neighbor 10.0.0.2  Source  10.0.0.1
    State: UP      (for 2d18h)
    Type: PASSIVE  (responding to requests)
    I/F: Et1/1
    LSPs protecting: 0
    Refresh Interval (msec) (used when ACTIVE)
      Configured: 100
      Statistics:
        Min:        0
        Max:        0
        Average:    0
        Waverage:   0
        Current:    0
    Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
    Counters:
      Communication with neighbor lost:
        Num times: 0
        Reasons:
          Missed acks:             0
          Bad Src_Inst received:   0
          Bad Dst_Inst received:   0
          I/F went down:           0
          Neighbor disabled Hello: 0
      Msgs Received:   2398194
           Sent:       2398195
           Suppressed: 0
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

clear ip rsvp hello instance statistics

To clear Hello statistics for an instance, use the **clear ip rsvp hello instance statistics** command in privileged EXEC mode.

clear ip rsvp hello instance statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not cleared for an instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.

Examples

This example shows sample output from the **show ip rsvp hello statistics** command and the values in those fields after you enter the **clear ip rsvp hello instance statistics** command.

```
Router# show ip rsvp hello statistics

  Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525

Router# clear ip rsvp hello instance statistics

Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:0
    Current length: 0 (max:500)
  Number of samples taken: 0
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

clear ip rsvp hello statistics

To globally clear Hello statistics, use the **clear ip rsvp hello statistics** command in privileged EXEC mode.

clear ip rsvp hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not globally cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2s	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.

Usage Guidelines

Use this command to remove all information about how long Hello packets have been in the Hello input queue.

Examples

Following is sample output from the **show ip rsvp hello statistics** command and the **clear ip rsvp hello statistics** command. Notice that the values in the "Packet arrival queue" fields have been cleared.

```
Router# show ip rsvp hello statistics

  Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525
```

```
Router# clear ip rsvp hello statistics

  Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:0
    Current length: 0 (max:500)
  Number of samples taken: 16
```

Related Commands

Command	Description
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

clear ip rsvp msg-pacing

To clear the Resource Reservation Protocol (RSVP) message pacing output from the **show ip rsvp neighbor** command, use the **clear ip rsvp msg-pacing** command in privileged EXEC mode.

clear ip rsvp msg-pacing

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears the RSVP message pacing output:

```
Router# clear ip rsvp msg-pacing
```

Related Commands

Command	Description
show ip rsvp counters	Displays counts of RSVP messages that were sent and received.
show ip rsvp neighbor	Displays the current RSVP neighbors and indicates whether the neighbor is using IP or UDP encapsulation for a specified interface or for all interfaces.

clear mpls counters

To clear the Multiprotocol Label Switching (MPLS) forwarding table disposition counters and the Any Transport over MPLS (AToM) imposition and disposition virtual circuit (VC) counters, use the **clear mpls counters** command in privileged EXEC mode.

clear mpls counters

Syntax Description

This command has no arguments or keywords.

Defaults

Checkpoint information resides on the active and standby Route Processor.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers. This command was updated to clear AToM VC counters.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

In the following example, the first **show mpls forwarding-table** command shows that 590 label-switched bytes exist in the forwarding table. The **clear mpls counters** command clears the counters. The second **show mpls forwarding-table** command shows that the number of label-switched bytes is 0.

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
20     30            10.10.17.17      590           Et3/0      172.16.0.2

Router# clear mpls counters

Clear "show mpls forwarding-table" counters [confirm]
mpls forward counters cleared

Router# show mpls forwarding-table

Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
20     30            10.10.17.17      0             Et3/0       172.16.0.2
```

In the following example, the first **show mpls l2 vc detail** command shows that 15 packets were received and sent, 1656 bytes were received, and 1986 bytes were sent. The **clear mpls counters** command clears the counters. The second **show mpls l2 transport vc detail** command shows that no bytes or packets were received or sent.

```
Router# show mpls l2 vc detail

Local interface: Et0/0.10 up, line protocol up, Eth VLAN 10 up
    MPLS VC type is Eth VLAN, interworking type is Ethernet
    Destination address: 10.0.0.2, VC ID: 10, VC status: up
        Output interface: Et1/0, imposed label stack {16}
        Preferred path: not configured
        Default path: active
        Next hop: 10.0.0.2
    Create time: 00:19:35, last status change time: 00:19:09
    Signaling protocol: LDP, peer 10.0.0.2:0 up
        MPLS VC labels: local 16, remote 16
        Group ID: local 0, remote 0
        MTU: local 1500, remote 1500
        Remote interface description:
    Sequencing: receive enabled, send enabled
    VC statistics:
        packet totals: receive 15, send 15 <---- packet totals
        byte totals:   receive 1656, send 1986 <---- byte totals
        packet drops:  receive 0, seq error 0, send 0

Router# clear mpls counters

Clear "show mpls forwarding-table" counters [confirm] mpls forward
counters cleared

Router# show mpls l2 vc detail

Local interface: Et0/0.10 up, line protocol up, Eth VLAN 10 up
    MPLS VC type is Eth VLAN, interworking type is Ethernet
    Destination address: 10.0.0.2, VC ID: 10, VC status: up
        Output interface: Et1/0, imposed label stack {16}
        Preferred path: not configured
        Default path: active
        Next hop: 10.0.0.2
    Create time: 00:22:55, last status change time: 00:22:29
    Signaling protocol: LDP, peer 10.0.0.2:0 up
        MPLS VC labels: local 16, remote 16
        Group ID: local 0, remote 0
        MTU: local 1500, remote 1500
        Remote interface description:
    Sequencing: receive enabled, send enabled
    VC statistics:
        packet totals: receive 0, send 0 <---- packet totals
        byte totals:   receive 0, send 0 <---- byte totals
        packet drops:  receive 0, seq error 0, send 0
```

Related Commands

Command	Description
show mpls forwarding-table	Displays the contents of the MPLS FIB.

clear mpls ip iprm counters

To clear the IP Rewrite Manager (IPRM) counters, use the **clear mpls ip iprm counters** command in privileged EXEC mode.

clear mpls ip iprm counters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command sets IPRM counters to zero.

Examples

The command in the following example clears the IPRM counters:

```
Router# clear mpls ip iprm counters

Clear iprm counters [confirm]
```

Related Commands

Command	Description
show mpls ip iprm counters	Displays the IPRM counters.

clear mpls ldp checkpoint

To clear the checkpoint information from the Label Information Base (LIB) entries on the active Route Processor (RP) or PRE and to clear the LIB entries created by checkpointing on the standby RP or PRE, use the **clear mpls ldp checkpoint** command in privileged EXEC mode.

clear mpls ldp checkpoint [**vrf** *vpn-name*] {**network** {*mask* | *length*} [**longer-prefixes**] | ***}** [**incomplete**]

Cisco 10000 Series Routers

clear mpls ldp checkpoint {**network** {*mask* | *length*} [**longer-prefixes**] | ***}** [**incomplete**]

Syntax Description

vrf *vpn-name*	(Optional) Clears the checkpoint information for the specified VPN routing and forwarding (VRF) instance (vpn-name). **Note** Applies to the Cisco 7000 series routers only.
network	Clears the checkpoint information for the specified destination address.
mask	Specifies the network mask, written as A.B.C.D.
length	Specifies the mask length.
longer-prefixes	(Optional) Clears the checkpoint information for any prefix that matches *mask* with the *length* specified.
*****	(Optional) Clears the checkpoint information for all destinations.
incomplete	(Optional) Clears any incomplete checkpoint information from the LIB.

Defaults

Checkpoint information resides on the active and standby RP.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.

Usage Guidelines

Use this command only when Cisco support personnel recommend it as a means of rectifying a problem.

On the active RP or PRE, this command does the following:

- Clears the checkpoint state information from the specified LIB entries.
- Triggers a checkpoint attempt for those entries.

On the standby RP or PRE, this command deletes all of the LIB entries created by checkpointing.

Examples

The command in the following example clears the checkpointing information for prefix 10.1.10.1:

```
Router(config)# clear mpls ldp checkpoint 10.1.10.1 32

Clear LDP bindings checkpoint state [confirm]

00:20:29: %LDP-5-CLEAR_CHKPT: Clear LDP bindings checkpoint state (*) by console
```

Related Commands

Command	Description
show mpls ldp checkpoint	Displays information about the LDP checkpoint system on the active RP.

clear mpls ldp neighbor

To forcibly reset a label distribution protocol (LDP) session, use the **clear mpls ldp neighbor** command in privileged EXEC mode.

clear mpls ldp neighbor [**vrf** *vpn-name*] {*nbr-address* | *****}

Syntax Description

vrf *vpn-name*	(Optional) Specifies the VPN routing and forwarding instance (*vpn-name*) for resetting an LDP session.
nbr-address	Specifies the address of the LDP neighbor whose session will be reset. The neighbor address is treated as <nbr-address>:0, which means it pertains to the LDP session for the LSR's platform-wide label space.
*****	Designates that all LDP sessions will be reset.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **clear mpls ldp neighbor** command terminates the specified LDP sessions. The LDP sessions should be reestablished if the LDP configuration remains unchanged.

You can clear an LDP session for an interface-specific label space of an LSR by issuing the **no mpls ip** command and then the **mpls ip** command on the interface associated with the LDP session.

Examples

The following example resets an LDP session:

```
Router# clear mpls ldp neighbor 10.12.12.12
```

To verify the results of the **clear mpls ldp neighbor** command, enter the **show mpls ldp neighbor** command. Notice the value in the "Up time" field.

```
Router# show mpls ldp neighbor 10.12.12.12

 Peer LDP Ident: 10.12.12.12:0; Local LDP Ident 10.13.13.13:0
   TCP connection: 10.12.12.12.646 - 10.13.13.13.15093
   State: Oper; Msgs sent/rcvd: 142/138; Downstream
   Up time: 02:16:28
   LDP discovery sources:
    Serial1/0, Src IP addr: 10.0.0.2
   Addresses bound to peer LDP Ident:
    10.0.0.129       10.12.12.12     10.0.0.2        10.1.0.5
    10.7.0.1
```

Then enter the following **clear mpls ldp neighbor 12.12.12.12** command. With mpls ldp logging configured, the easiest way to verify the **clear mpls ldp neighbor** command is to monitor the LDP log messages.

```
Router# clear mpls ldp neighbor 10.12.12.12

1w1d: %LDP-5-CLEAR_NBRS: Clear LDP neighbors (10.12.12.12) by console
1w1d: %LDP-5-NBRCHG: LDP Neighbor 10.12.12.12:0 is DOWN
1w1d: %LDP-5-NBRCHG: LDP Neighbor 10.12.12.12:0 is UP
```

Reenter the **show mpls ldp neighbor 10.12.12.12** command. Notice that the "Up time" value has been reset.

```
Router# show mpls ldp neighbor 10.12.12.12

  Peer LDP Ident: 10.12.12.12:0; Local LDP Ident 10.13.13.13:0
    TCP connection: 10.12.12.12.646 - 10.13.13.13.15095
    State: Oper; Msgs sent/rcvd: 125/121; Downstream
    Up time: 00:00:05
    LDP discovery sources:
     Serial1/0, Src IP addr: 10.0.0.2
    Addresses bound to peer LDP Ident:
     10.0.0.129       10.12.12.12     10.0.0.2        10.1.0.5
     10.7.0.1
```

The following example resets all LDP sessions:

```
Router# clear mpls ldp neighbor *
```

Related Commands

Command	Description
show mpls ldp neighbor	Displays the status of the LDP sessions.

clear mpls traffic-eng auto-bw timers

To reinitialize the automatic bandwidth adjustment feature on a platform, use the **clear mpls traffic-eng auto-bw timers** command in user EXEC mode.

clear mpls traffic-eng auto-bw timers

Syntax Description

This command has no arguments or keywords.

Defaults

There are no defaults for this command.

Command Modes

User EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For each tunnel for which automatic bandwidth adjustment is enabled, the platform maintains information about sampled output rates and the time remaining until the next bandwidth adjustment. The **clear mpls traffic-eng auto-bw timers** command clears this information for all such tunnels. The effect is as if automatic bandwidth adjustment had just been enabled for the tunnels.

Examples

The following example shows how to clear information about sampled output rates and the time remaining until the next bandwidth adjustment:

```
Router# clear mpls traffic-eng auto-bw timers

Clear mpls traffic engineering auto-bw timers [confirm]
```

Related Commands

Command	Description
mpls traffic-eng auto-bw timers	Enables automatic bandwidth adjustment on a platform for tunnels configured for bandwidth adjustment.
tunnel mpls traffic-eng auto-bw	Enables automatic bandwidth adjustment for a tunnel, specifies the frequency with which tunnel bandwidth can be automatically adjusted, and designates the allowable range of bandwidth adjustments.

clear mpls traffic-eng auto-tunnel mesh

To remove all mesh tunnel interfaces and re-create them, use the **clear mpls traffic-eng auto-tunnel mesh** command in privileged EXEC mode.

clear mpls traffic-eng auto-tunnel mesh

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example shows how to remove all mesh tunnel interfaces and re-create them:

```
Router# clear mpls traffic-eng auto-tunnel mesh
```

Related Commands

Command	Description
interface auto-template	Creates the template interface.

clear mpls traffic-eng auto-tunnel backup

To remove all the backup autotunnels and re-create them, use the **clear mpls traffic-eng auto-tunnel backup** command in global configuration mode.

clear mpls traffic-eng auto-tunnel backup

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example removes all backup autotunnels and re-creates them:

```
Router# clear mpls traffic-eng auto-tunnel backup
```

Related Commands

Command	Description
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

clear mpls traffic-eng auto-tunnel primary

To remove all the primary autotunnels and re-create them, use the **clear mpls traffic-eng auto-tunnel primary** command in global configuration mode.

clear mpls traffic-eng auto-tunnel primary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example removes all primary autotunnels and re-creates them:

```
Router# clear mpls traffic-eng auto-tunnel primary
```

Related Commands

Command	Description
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

clear mpls traffic-eng tunnel counters

To clear the counters for all Multiprotocol Label Switching (MPLS) traffic engineering tunnels, use the **clear mpls traffic-eng tunnel counters** command in privileged EXEC mode.

clear mpls traffic-eng tunnel counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command allows you to set the MPLS traffic engineering tunnel counters to zero so that you can see changes to the counters easily.

Examples

In the following example, the counters for all MPLS traffic engineering tunnels are cleared and a request is made for confirmation that the specified action occurred:

```
Router# clear mpls traffic-eng tunnel counters

Clear traffic engineering tunnel counters [confirm]
```

Related Commands

Command	Description
show mpls traffic-eng tunnels statistics	Displays event counters for one or more MPLS traffic engineering tunnels.

clear xconnect

To remove xconnect attachment circuits and pseudowires, use the **clear xconnect** command in privileged EXEC configuration mode.

clear xconnect {**all | interface** *interface* **| peer** *ip-address* {**all** | **vcid** *vc-id*}}

Syntax Description

all	Removes all xconnect attachment circuits and pseudowires.
interface *interface*	Removes xconnect attachment circuits and pseudowires on the specified interface.
peer *ip-address* {**all** | **vcid** *vc-id*}	Removes xconnect attachment circuits and pseudowires associated with the specified peer IP address. • **all**—Removes all xconnects associated with the specified peer IP address. • **vcid** *vcid*—Removes xconnects associated with the specified peer IP address and the specified VCID.

Command Default

xconnect attachment circuits and pseudowires are not removed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example removes all xconnects:

```
Router# clear xconnect all

02:13:56: Xconnect[ac:Et1/0.1(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:13:56: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=2
02:13:56: Xconnect[ac:Et1/0.2(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:13:56: Xconnect[mpls:10.1.1.2:1234001]: provisioning fwder with fwd_type=2, sss_role=1
02:13:56: Xconnect[ac:Et1/0.3(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:13:56: Xconnect[mpls:10.1.2.2:1234002]: provisioning fwder with fwd_type=2, sss_role=2
02:13:56: Xconnect[ac:Et1/0.4(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:13:56: Xconnect[mpls:10.1.2.2:1234003]: provisioning fwder with fwd_type=2, sss_role=1
02:13:56: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:13:56: MPLS peer 10.1.1.2 vcid 1234001, VC DOWN, VC state DOWN
02:13:56: MPLS peer 10.1.2.2 vcid 1234002, VC DOWN, VC state DOWN
02:13:56: MPLS peer 10.1.2.2 vcid 1234003, VC DOWN, VC state DOWN
02:13:56: XC AUTH [Et1/0.1, 1001]: Event: start xconnect authorization, state changed from
IDLE to AUTHORIZING
02:13:56: XC AUTH [Et1/0.1, 1001]: Event: found xconnect authorization, state changed from
AUTHORIZING to DONE
02:13:56: XC AUTH [Et1/0.3, 1003]: Event: start xconnect authorization, state changed from
IDLE to AUTHORIZING
02:13:56: XC AUTH [Et1/0.3, 1003]: Event: found xconnect authorization, state changed from
AUTHORIZING to DONE
```

```
02:13:56: XC AUTH [10.1.1.2, 1234001]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:13:56: XC AUTH [10.1.1.2, 1234001]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:13:56: XC AUTH [10.1.2.2, 1234003]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:13:56: XC AUTH [10.1.2.2, 1234003]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:13:56: XC AUTH [Et1/0.1, 1001]: Event: free xconnect authorization request, state
changed from DONE to END
02:13:56: XC AUTH [Et1/0.3, 1003]: Event: free xconnect authorization request, state
changed from DONE to END
02:13:56: XC AUTH [10.1.1.2, 1234001]: Event: free xconnect authorization request, state
changed from DONE to END
02:13:56: XC AUTH [10.1.2.2, 1234003]: Event: free xconnect authorization request, state
changed from DONE to END
02:13:56: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
02:13:56: MPLS peer 10.1.2.2 vcid 1234003, VC UP, VC state UP
02:13:56: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP
02:13:56: MPLS peer 10.1.2.2 vcid 1234002, VC UP, VC state UP
```

The following example removes all the xconnects associated with peer router 10.1.1.2:

```
Router# clear xconnect peer 10.1.1.2 all

02:14:08: Xconnect[ac:Et1/0.1(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:14:08: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=2
02:14:08: Xconnect[ac:Et1/0.2(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:14:08: Xconnect[mpls:10.1.1.2:1234001]: provisioning fwder with fwd_type=2, sss_role=1
02:14:08: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:14:08: MPLS peer 10.1.1.2 vcid 1234001, VC DOWN, VC state DOWN
02:14:08: XC AUTH [Et1/0.1, 1001]: Event: start xconnect authorization, state changed from
IDLE to AUTHORIZING
02:14:08: XC AUTH [Et1/0.1, 1001]: Event: found xconnect authorization, state changed from
AUTHORIZING to DONE
02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:14:08: XC AUTH [Et1/0.1, 1001]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:08: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
02:14:08: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP
```

The following example removes the xconnects associated with peer router 10.1.1.2 and VC ID 1234001:

```
Router# clear xconnect peer 10.1.1.2 vcid 1234001

02:14:23: Xconnect[ac:Et1/0.2(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=1
02:14:23: Xconnect[mpls:10.1.1.2:1234001]: provisioning fwder with fwd_type=2, sss_role=2
02:14:23: MPLS peer 10.1.1.2 vcid 1234001, VC DOWN, VC state DOWN
02:14:23: XC AUTH [Et1/0.2, 1002]: Event: start xconnect authorization, state changed from
IDLE to AUTHORIZING
02:14:23: XC AUTH [Et1/0.2, 1002]: Event: found xconnect authorization, state changed from
AUTHORIZING to DONE
02:14:23: XC AUTH [Et1/0.2, 1002]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:23: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
```

The following example removes the xconnects associated with interface Ethernet 1/0.1:

```
Router# clear xconnect interface eth1/0.1

02:14:48: Xconnect[ac:Et1/0.1(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
```

```
02:14:48: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=1
02:14:48: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:48: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP
```

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and pseudowires,

connect (Frame Relay)

To define connections between Frame Relay permanent virtual circuits (PVCs), use the **connect** command in global configuration mode. To remove connections, use the **no** form of this command.

connect *connection-name interface dlci* {*interface dlci* | **l2transport**}

no connect *connection-name interface dlci* {*interface dlci* | **l2transport**}

Syntax Description

connection-name	A name for this connection.
interface	Interface on which a PVC connection will be defined.
dlci	Data-link connection identifier (DLCI) number of the PVC that will be connected.
l2transport	Specifies that the PVC will not be a locally switched PVC, but will be tunneled over the backbone network.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.0(23)S	The **l2transport** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When Frame Relay switching is enabled, the **connect** command creates switched PVCs in Frame Relay networks.

Examples

The following example shows how to define a connection called “frompls1” with DLCI 100 on serial interface 5/0.

```
connect frompls1 Serial5/0 100 l2transport
```

The following example shows how to enable Frame Relay switching and define a connection called "one" between DLCI 16 on serial interface 0 and DLCI 100 on serial interface 1.

```
frame-relay switching
connect one serial0 16 serial1 100
```

Related Commands

Command	Description
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
mpls l2transport route	Enables routing of Frame Relay packets over a specified VC.

connect (L2VPN local switching)

To create Layer 2 data connections between two ports on the same router, use the **connect** command in global configuration mode. To remove such connections, use the **no** form of this command.

Syntax for 12.0S, 12.2S and 12.4T Releases

connect *connection-name type number* [*dlci* | *pvc* | *pvp*] *type number* [*dlci* | *pvc* | *pvp*] [**interworking ip** | **ethernet**]

no connect *connection-name type number* [*dlci* | *pvc* | *pvp*] *type number* [*dlci* | *pvc* | *pvp*] [**interworking ip** | **ethernet**]

Syntax for Cisco IOS XE Release 2.5 and Later Releases

connect *connection-name type number type number*

no connect *connection-name type number type number*

Syntax Description

connection-name	A name for this local switching connection.
type	String that identifies the type of interface used to create a local switching connection; for example, serial or Gigabit Ethernet.
number	Integer that identifies the number of the interface; for example, 0/0/0.1 for a Gigabit Ethernet interface.
dlci	(Optional) The data-link connection identifier (DLCI) assigned to the interface.
pvc	(Optional) The permanent virtual circuit (PVC) assigned to the interface, expressed by its vpi/vci (virtual path and virtual channel identifiers).
pvp	(Optional) The permanent virtual path (PVP) assigned to the interface.
interworking ip | **ethernet**	(Optional) Specifies that this local connection enables different transport types to be switched locally. These keyword options are not necessary for configurations that locally switch the same transport type, such as ATM to ATM, or Frame Relay to Frame Relay. Choices are: • **interworking ip**—Causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. Attachment circuit frames that do not contain IPv4 packets are dropped. • **ethernet**—Causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, leaving a pure Ethernet frame.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced for local switching.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following example shows an Ethernet interface configured for Ethernet, plus an ATM interface configured for AAL5 Subnetwork Access Protocol (SNAP) encapsulation. The **connect** command allows local switching between these two interfaces and specifies the interworking type as IP mode.

```
Router(config)# interface atm 0/0/0
Router(config-if)# pvc 0/100 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5snap

Router(config)# interface fastethernet 6/0/0.1
Router(config-subif)# encapsulation dot1q 100

Router(config)# connect atm-eth-con atm 0/0/0 0/100 fastethernet 6/0/0.1 interworking ip
```

Related Commands

Command	Description
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.

context

To associate a Simple Network Management Protocol (SNMP) context with a particular virtual private network (VPN) routing and forwarding (VRF) instance, use the **context** command in VRF configuration mode. To disassociate an SNMP context from a VPN, use the **no** form of this command.

context *context-name*

no context *context-name*

Syntax Description

context-name	Name of the SNMP VPN context, up to 32 characters.

Command Default

No SNMP contexts are associated with VPNs.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for IPv6 was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Before you use this command to associate an SNMP context with a VPN, you must do the following:

- Issue the **snmp-server context** command to create an SNMP context
- Associate a VPN with a context so that the specific MIB data for that VPN exists in that context.
- Associate a VPN group with the context of the VPN using the **snmp-server group** command with the **context** *context-name* keyword and argument.

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, MIB data for that VPN exists in that context. Associating a VPN with a context helps enable 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.

A route distinguisher (RD) is required when you configure an SNMP context. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of a IPv4 prefix to make it globally unique. An RD is either ASN relative, which means it is composed of an autonomous system number and an arbitrary number, or it is IP address relative and composed of an IP address and an arbitrary number.

Examples

The following example shows how to create an SNMP context named context1 and associate the context with the VRF named vrf1:

```
Router(config)# snmp-server context1
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:120
Router(config-vrf)# context context1
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode for the configuration of a VRF.
snmp mib community-map	Associates an SNMP community with an SNMP context, engine ID, or security name.
snmp mib target list	Creates a list of target VRFs and hosts to associate with an SNMP v1 or v2c community.
snmp-server context	Creates an SNMP context.
snmp-server group	Configures a new SNMP group, or a table that maps SNMP users to SNMP views.
snmp-server trap authentication vrf	Controls VRF-specific SNMP authentication failure notifications.
snmp-server user	Configures a new user to an SNMP group.

control-word

To enable the Multiprotocol Label Switching (MPLS) control word in an Any Transport over MPLS (AToM) dynamic pseudowire connection, use the **control-word** command in pseudowire class configuration mode. To set the control word to autosense mode, use the **default control-word** command. To disable the control word, use the **no** form of this command.

control-word

default control-word

no control-word

Syntax Description

This command has no arguments or keywords.

Command Default

The control word is set to autosense mode.

Command Modes

Pseudowire class configuration (config-pw-class)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

If the MPLS control word is enabled for a static pseudowire and you disable it at the xconnect level, any option set by the pseudowire class is disabled.

Examples

The following example shows how to enable the control word in an AToM dynamic pseudowire connection:

```
Router# configure terminal
Router(config)# pseudowire-class cw_enable
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# control-word
Router(config-pw-class)# exit
```

The following example shows how to enable the control word in an AToM dynamic pseudowire connection and set it to autosense mode:

```
Router# configure terminal
Router(config)# pseudowire-class cw_enable
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# default control-word
Router(config-pw-class)# exit
```

Related Commands

Command	Description
mpls control-word	Enables the MPLS control word in an AToM static pseudowire connection.
show mpls l2transport binding	Displays VC label binding information.
show mpls l2transport vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.
xconnect	Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.

description (l2 vfi)

To provide a description of the switching provider edge (PE) router for an L2VPN multisegment pseudowire, use the **description** command in L2 VFI configuration mode. To remove the description, use the **no** form of this command.

description *string*

no description *string*

Syntax Description

string	Switching PE router description. The string must be 80 characters or fewer.

Command Default

The switching PE router does not have a description.

Command Modes

L2 VFI (config-vfi)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.

Usage Guidelines

This description is useful for tracking the status of each switching PE router.

Examples

This example adds a description for switching PE router 2:

```
Router(config)# l2 vfi domain_a point-to-point
Router(config-vfi)# description s-pe2
```

Related Commands

Command	Description
show mpls l2 transport vc detail	Displays the status information about the pseudowire, including the switching PE router.

echo

To customize the default behavior of echo packets, use the **echo** command in MPLS OAM configuration mode. To set the echo packet's behavior to its default value, use the **no** form of this command.

echo {**revision** {**3** | **4**} | **vendor-extension**}

no echo {**revision** {**3** | **4**} | **vendor-extension**}

Syntax Description

revision	Specifies the revision number of the echo packet's default values. Valid values are: • **3**—draft-ietf-mpls-lsp-ping-03 (Revision 2) • **4**—RFC 4379 compliant (default)
vendor-extension	Sends Cisco-specific extension of type, length, values (TLVs) with echo packets.

Command Default

Cisco-specific extension TLVs are sent with the echo packet. Revision 4 is the router's default.

Command Modes

MPLS OAM configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Before you can enter the **echo** command, you must first enter the **mpls oam** command to enter MPLS OAM configuration mode.

Specify the **revision** keyword only if one of the following conditions exists:

- You want to change the revision number from the default of revision **4** to revision **3**.
- You previously entered the **mpls oam** command and changed the revision number to **3** and now you want to change the revision back to **4**.

To prevent failures reported by the replying router due to TLV version issues, you can use the **echo revision** command to configure all routers in the core for the same version of the Internet Engineering Task Force (IEFT) label switched paths (LSP) ping draft. For example, if the network is running draft RFC 4379 implementations, but one router is capable of only Version 3 (Cisco Revision 3), configure all

routers in the network to operate in Revision 3 mode. Revision 3 mode is used only with Multiprotocol Label Switching (MPLS) LSP ping or traceroute. Revision 3 mode does not support MPLS multipath LSP traceroute.

The **vendor-extension** keyword is enabled by default in the router. If your network includes routers that are not Cisco routers, you may want to disable Cisco extended TLVs. To disable Cisco extended TLVs, specify the **no echo vendor-extension** command in MPLS OAM configuration mode. To enable Cisco extended TLVs again, respecify the **echo** command with the **vendor-extension** keyword.

Examples

The following example uses Revision 3 of the echo packets and sends the vendor's extension TLV with the echo packet:

```
mpls oam
 echo revision 3
 echo vendor-extension
 exit
```

Related Commands

Command	Description
mpls oam	Enters MPLS OAM configuration mode for customizing the default behavior of echo packets.

encapsulation (Any Transport over MPLS)

To configure the ATM adaptation layer (AAL) encapsulation for an Any Transport over MPLS (AToM), use the **encapsulation** command in the appropriate configuration mode. To remove the ATM encapsulation, use the **no** form of this command.

encapsulation *layer-type*

no encapsulation *layer-type*

Syntax Description

layer-type	The adaptation layer type, which is one of the following: • **aal5**—ATM adaptation layer 5 • **aal0**—ATM adaptation layer 0

Command Default

The default encapsulation is AAL5.

Command Modes

L2transport VC configuration—for ATM PVCs
VC class configuration—for VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable ATM encapsulations as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

In L2transport VC configuration mode, the **pvc** command and the **encapsulation** command work together. Use the commands for AToM differently than for all other applications. Table 8 shows the differences in how the commands are used.

Table 8 AToM-Specific Variations of the pvc and encapsulation Commands

Other Applications	AToM
`Router(config-if)# pvc 1/100` `Router(config-if-atm-vc)# encapsulation aal5snap`	`Router(config-if)# pvc 1/100 l2transport` `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`

The following list highlights the differences:

- **pvc** command: For most applications, you create a permanent virtual circuit (PVC) by using the **pvc** *vpi/vci* command. For AToM, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- **encapsulation** command: The **encapsulation** command for AToM has only two keyword values: **aal5** or **aal0**. You cannot specify an encapsulation type, such as aal5snap. In contrast, the **encapsulation aal5** command you use for most other applications requires you to specify the encapsulation type, such as **aal5snap**.
- You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets.

When you use the **aal5** keyword, incoming cells (except Operation, Administration, and Maintenance [OAM] cells) on that PVC are treated as AAL5 encapsulated packets. The router reassembles the packet from the incoming cells. The router does not check the contents of the packet, so it does not need to know the encapsulation type (such as aal5snap and aal5mux). After imposing the Multiprotocol Label Switching (MPLS) label stack, the router sends the reassembled packet over the MPLS core network.

When you use the **aal0** keyword, the router strips the header error control (HEC) byte from the cell header and adds the MPLS label stack. The router sends the cell over the MPLS core network.

Examples

The following example shows how to configure a PVC to transport ATM cell relay packets for AToM:

```
Router> enable
Router# configure terminal
Router(config)# interface atm1/0
Router(config-if)# pvc 1/100 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aal0
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example shows how to configure ATM AAL5 over MPLS in VC class configuration mode. The VC class is applied to a PVC.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm aal5class
Router(config-vc-class)# encapsulation aal5
Router(config)# interface atm1/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# class-vc aal5class
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation (Layer 2 local switching)

To configure the ATM adaptation layer (AAL) for a Layer 2 local switching ATM permanent virtual circuit (PVC), use the **encapsulation** command in ATM PVC L2transport configuration mode. To remove an encapsulation from a PVC, use the **no** form of this command.

encapsulation *layer-type*

no encapsulation *layer-type*

Syntax Description

layer-type	Adaptation layer type. The values are: • **aal5** • **aal0** • **aal5snap** • **aal5mux** • **aal5nlpid** (not available on Cisco 12000 series)

Command Default

If you do not create a PVC, one is created for you. The default encapsulation types for autoprovisioned PVCs are as follows:

- For ATM-to-ATM local switching, the default encapsulation type for the PVC is AAL0.
- For ATM-to-Ethernet or ATM-to-Frame Relay local switching, the default encapsulation type for the PVC is AAL5SNAP.

Command Modes

ATM PVC L2transport configuration

Command History

Release	Modification
12.0(27)S	This command was introduced for Layer 2 local switching.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **pvc** command and the **encapsulation** command work together. The use of these commands with Layer 2 local switching is slightly different from the use of these commands with other applications. The following list highlights the differences:

- For Layer 2 local switching, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- The Layer 2 local switching **encapsulation** command works only with the **pvc** command. You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets. You can use only PVCs to transport Layer 2 packets.

Table 9 shows the encapsulation types supported for each transport type:

Table 9 Supported Encapsulation Types

Interworking Type	Encapsulation Type
ATM to ATM	AAL0, AAL5
ATM to Ethernet with IP interworking	AAL5SNAP, AAL5MUX
ATM to Ethernet with Ethernet interworking	AAL5SNAP
ATM to Frame-Relay	AAL5SNAP, AAL5NLPID

Examples

The following example shows how to configure a PVC to transport AAL0 packets for Layer 2 local switching:

```
pvc 1/100 l2transport
 encapsulation aal0
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN), use the **encapsulation dot1q** command in interface range configuration mode or subinterface configuration mode. To disable IEEE 802.1Q encapsulation, use the **no** form of this command.

Interface Range Configuration Mode

encapsulation dot1q *vlan-id* [**native**]

no encapsulation dot1q

Subinterface Configuration Mode

encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id-vlan-id*[**,***vlan-id-vlan-id*]}

no encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id-vlan-id*[**,***vlan-id-vlan-id*]}

Syntax Description

vlan-id	Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID.
native	(Optional) Sets the VLAN ID value of the port to the value specified by the *vlan-id* argument. **Note** This keyword is not supported by the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
second-dot1q	Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature by allowing an inner VLAN ID to be configured.
any	Sets the inner VLAN ID value to a number that is not configured on any other subinterface. **Note** The **any** keyword in the **second-dot1q** command is not supported on a subinterface configured for IP over Q-in-Q (IPoQ-in-Q) because IP routing is not supported on ambiguous subinterfaces.
-	Hyphen must be entered to separate inner and outer VLAN ID values that are used to define a range of VLAN IDs.
,	(Optional) Comma must be entered to separate each VLAN ID range from the next range.

Defaults

IEEE 802.1Q encapsulation is disabled.

Command Modes

Interface range configuration
Subinterface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The **native** keyword was added.
12.2(2)DD	Configuration of this command in interface range mode was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(7)T	The **second-dot1q** keyword was added to support the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

Interface Range Configuration Mode

IEEE 802.1Q encapsulation is configurable on Fast Ethernet interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Use the **encapsulation dot1q** command in interface range configuration mode to apply a VLAN ID to each subinterface within the range specified by the **interface range** command. The VLAN ID specified by the *vlan-id* argument is applied to the first subinterface in the range. Each subsequent interface is assigned a VLAN ID, which is the specified *vlan-id* plus the subinterface number minus the first subinterface number (VLAN ID + subinterface number – first subinterface number).

Note The Cisco 10000 series router does not support the **interface range** command nor the interface range configuration mode.

Do not configure encapsulation on the native VLAN of an IEEE 802.1Q trunk without using the **native** keyword. (Always use the **native** keyword when *vlan-id* is the ID of the IEEE 802.1Q native VLAN.)

Subinterface Configuration Mode

Use the **second-dot1q** keyword to configure the IEEE 802.1Q-in-Q VLAN Tag Termination feature. 802.1Q in 802.1Q (Q-in-Q) VLAN tag termination adds another layer of 802.1Q tag (called “metro tag” or “PE-VLAN”) to the 802.1Q tagged packets that enter the network. Double tagging expands the VLAN space, allowing service providers to offer certain services such as Internet access on specific VLANs for some customers and other types of services on other VLANs for other customers.

After a subinterface is defined, use the **encapsulation dot1q** command to add outer and inner VLAN ID tags to allow one VLAN to support multiple VLANs. You can assign a specific inner VLAN ID to the subinterface; that subinterface is unambiguous. Or you can assign a range or ranges of inner VLAN IDs to the subinterface; that subinterface is ambiguous.

Examples

The following example shows how to create the subinterfaces within the range 0.11 and 0.60 and apply VLAN ID 101 to the Fast Ethernet0/0.11 subinterface, VLAN ID 102 to Fast Ethernet0/0.12 (*vlan-id* = 101 + 12 – 11 = 102), and so on up to VLAN ID 150 to Fast Ethernet0/0.60 (*vlan-id* = 101 + 60 – 11 = 150):

```
Router(config)# interface range fastethernet0/0.11 - fastethernet0/0.60
Router(config-int-range)# encapsulation dot1q 101
```

The following example shows how to terminate a Q-in-Q frame on an unambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID of 200:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
```

The following example shows how to terminate a Q-in-Q frame on an ambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID in the range from 100 to 199 or from 201 to 600:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600
```

Related Commands

Command	Description
encapsulation isl	Enables the ISL, which is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches.
encapsulation sde	Enables IEEE 802.10 encapsulation of traffic on a specified subinterface in VLANs.
interface range	Specifies multiple subinterfaces on which subsequent commands are executed at the same time.
show vlans dot1q	Displays information about 802.1Q VLAN subinterfaces.

encapsulation mpls

To specify that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire, use the **encapsulation mpls** command in pseudowire class configuration mode. To remove MPLS as the encapsulation method, use the **no pseudowire-class** command.

encapsulation mpls

no pseudowire-class

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Pseudowire class configuration

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

You must specify **encapsulation mpls** as part of the **xconnect** command or as part of a pseudowire class for the AToM VCs to work properly.

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 re-establish the pseudowire and specify the new encapsulation type.

Examples

The following example shows how to configure MPLS as the data encapsulation method for the pseudowire class ether-pw:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation mpls
```

Related Commands

Command	Description
encapsulation l2tpv3	Configures L2TPv3 as the data encapsulation method over IP networks.
pseudowire-class	Specifies the name of a pseudowire class and enters pseudowire class configuration mode.

exclude-address

To exclude an address from an IP explicit path, use the **exclude-address** command in global configuration mode after entering explicit path configuration mode via the **ip-explicit path** command. To remove an address exclusion from an IP explicit path, use the **no index** command.

exclude-address *A.B.C.D*

no index *number*

Syntax Description

A.B.C.D	Excludes an address from subsequent partial path segments. You can enter the IP address of a link or the router ID of a node.
number	Removes the specified address exclusion from an IP explicit path.

Defaults

Addresses are not excluded from an IP explicit path unless explicitly excluded by the **exclude-address** command.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. If you enter the **exclude-address** command and specify the IP address of a link, the constraint-based Shortest Path First (SPF) routine does not consider that link when it sets up Multiprotocol Label Switching (MPLS) traffic engineering paths. If the excluded address is a flooded MPLS traffic engineering router ID, the constraint-based SPF routine does not consider that entire node. The person performing the configuration must know the router IDs of the routers because it will not be apparent whether the specified number is for a link or for a node.

Note MPLS traffic engineering will accept an IP explicit path that comprises 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.

Examples

The following example shows how to exclude IP addresses 10.0.0.125 and 10.0.0.135 from IP explicit path 500:

```
Router(config-ip-expl-path)# exclude-address 10.0.0.125
Explicit Path identifier 500:
       1: exclude-address 10.0.0.125
Router(config-ip-expl-path)# exclude-address 10.0.0.135
Explicit Path identifier 500:
       1: exclude-address 10.0.0.125
       2: exclude-address 10.0.0.135
Router(config-ip-expl-path)# end
```

To remove IP address 10.0.0.135 from the excluded addresses for explicit path 500, use the following commands:

```
Router(config)# ip explicit-path identifier 500
Router(cfg-ip-expl-path)# no index 1
Explicit Path identifier 500:
    2: exclude-address 10.0.0.135
Router(cfg-ip-expl-path)# end
```

Related Commands

Command	Description
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies a specified path.

exit (LSP Attributes)

To exit from the label switched path (LSP) attribute list, use the **exit** command in LSP Attributes configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command after you have configured LSP-related attributes for a traffic engineering (TE) tunnel to exit the LSP attribute list and the LSP Attributes configuration mode.

Examples

The following example shows how to set up an LSP attribute list and exit the LSP Attributes configuration mode when the list is complete:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# priority 7 7
Router(config-lsp-attr)# affinity 0 0
Router(config-lsp-attr)# exit
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

exit-address-family

To exit from address family configuration mode, use the **exit-address-family** command in address family configuration mode.

exit-address-family

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Address family configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) support was added in Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	EIGRP support was added in Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP support was added.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is used to exit address family configuration mode.

This command can be abbreviated to **exit**.

Examples

In the following example, the router is configured to exit address family configuration mode:

```
Router(config-router-af)# exit-address-family
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode.
address-family ipv6	Enters IPv6 address family configuration mode.
address-family nsap	Enters CLNS address family configuration mode.
address-family vpnv4	Enters VPNv4 address family configuration mode.

exp

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **exp** command in Frame Relay VC-bundle-member configuration mode. To remove the EXP level configuration from the PVC, use the **no** form of this command.

exp {*level* | **other**}

no exp

Syntax Description

level	The MPLS EXP level or levels for this Frame Relay PVC bundle member. The range is from 0 to 7. A PVC bundle member can be configured with a single level, multiple individual levels, a range of levels, multiple ranges of levels, or a combination of individual levels and level ranges. Levels can be specified in ascending or descending order (although a subsequent **show running-config** command will display them in ascending order). Examples are as follows: • 0 • 0,2,3 • 6-5 • 0-2,4-5 • 0,1,2-4,7
other	Specifies that this Frame Relay PVC bundle member will handle all of the remaining MPLS EXP levels that are not explicitly configured on any other bundle member PVCs.

Defaults

EXP levels are not configured.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(16)BX	This command was integrated into Cisco IOS Release 12.2(16)BX.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Assignment of MPLS EXP levels to Frame Relay PVC bundle members lets you create differentiated services, because you can distribute the levels over the various PVC bundle members. You can map a single level or a range of levels to each discrete PVC in the bundle, which enables PVCs in the bundle to carry packets marked with different levels.

Use the **exp other** command to indicate that a PVC can carry traffic marked with EXP levels not specifically configured for other PVCs. Only one PVC in the bundle can be configured using the **exp other** command.

All EXP levels must be accounted for in the PVC bundle configuration, or the bundle will not come up. However, a PVC can be a bundle member but have no EXP level associated with it. As long as all valid EXP levels are handled by other PVCs in the bundle, the bundle can come up, but the PVC that has no EXP level configured will not participate in it.

The **exp** command is available only when MPLS is configured on the interface with the **mpls ip** command.

You can overwrite the EXP level configuration on a PVC by reentering the **exp** command with a new value.

The MPLS experimental bits are a bit-by-bit copy of the IP precedence bits. When Frame Relay PVC bundles are configured for IP precedence and MPLS is enabled, the **precedence** command is replaced by the **exp** command. When MPLS is disabled, the **exp** command is replaced by the **precedence** command.

Examples

The following example shows the configuration of four Frame Relay PVC bundle members in PVC bundle bundle1 configured with MPLS EXP level support:

```
interface serial 0.1 point-to-point
 encapsulation frame-relay
 ip address 10.1.1.1
 mpls ip
 frame-relay vc-bundle bundle1
 pvc 100 ny-control
 class control
 exp 7
 protect vc
 pvc 101 ny-premium
 class premium
 exp 6-5
 protect group
 no bump traffic
 bump explicit 7
 pvc 102 my-priority
 class priority
 exp 4-2
 protect group
 pvc 103 ny-basic
 class basic
 exp other
 protect group
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
class	Associates a map class with a specified DLCI.

Command	Description
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members.
mpls ip	Enables label switching of IPv4 packets on an interface.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.
protect	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.

export map

To associate an export map with a VPN Routing and Forwarding (VRF) instance, use the **export map** command in IP VRF configuration mode.

export map *route-map*

no export map *route-map*

Syntax Description

route-map	Specifies the route map to be used as an export map.

Command Default

No export maps are associated with a VRF instance.

Command Modes

IP VRF configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **export map** command is used to associate a route map with the specified VRF. The export map is used to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route. Only one export route map can be configured for a VRF.

An export route map can be used when an application requires finer control over the routes that are exported out of a VRF than the control that is provided by import and export extended communities configured for the importing and exporting VRFs.

Examples

In the following example, an export is configured under the VRF and an access list and route map are configured to specify which prefixes are exported:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# export map BLUE
Router(config-vrf)# route-target import 2:1
Router(config-vrf)# exit
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# route-map BLUE permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set extcommunity rt 2:1
Router(config-route-map)# end
```

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

extended-port

Note Effective with Cisco IOS Release 12.4(20)T, the **extended-port** command is not available in Cisco IOS software.

To associate the currently selected extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface with a particular external interface on the remotely controlled ATM switch, use the **extended-port** command in interface configuration mode.

extended-port *ctrl-if* {**bpx** *bpx-port-number* | **descriptor** *vsi-descriptor* | **vsi** *vsi-port-number*}

Syntax Description

ctrl-if	Identifies the ATM interface used to control the remote ATM switch. You must configure Virtual Switch Interface (VSI) on this interface using the **label-control-protocol** interface configuration command.
bpx *bpx-port-number*	Specifies the associated Cisco BPX interface using the native BPX syntax. *slot.port* [.*virtual port*] You can use this form of the command only when the controlled switch is a Cisco BPX switch.
descriptor *vsi-descriptor*	Specifies the associated port by its VSI physical descriptor. The *vsi-descriptor* string must match the corresponding VSI physical descriptor.
vsi *vsi-port-number*	Specifies the associated port by its VSI port number. The *vsi-port-number* string must match the corresponding VSI physical port number.

Defaults

Extended MPLS ATM interfaces are not associated.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

The **extended-port** interface configuration command associates an XTagATM interface with a particular external interface on the remotely controlled ATM switch. The three alternate forms of the command permit the external interface on the controlled ATM switch to be specified in three different ways.

Examples

The following example shows how to associate an extended MPLS ATM interface and bind it to BPX port 2.3:

```
ATM(config)# interface XTagATM23
ATM(config-if)# extended-port atm0/0 bpx 2.3
```

The following example shows how to associate an extended MPLS ATM interface and bind it to port 2.4:

```
ATM(config)# interface XTagATM24
ATM(config-if)# extended-port atm0/0 descriptor 0.2.4.0
```

The following example shows how to associate an extended MPLS ATM interface and binds it to port 1622:

```
ATM(config)# interface XTagATM1622
ATM(config-if)# extended-port atm0/0 vsi 0x00010614
```

Related Commands

Command	Description
interface XTagATM	Enters interface configuration mode for an extended MPLS ATM (XTagATM) interface.
show controller vsi status	Displays a summary of each VSI-controlled interface.

forward permit l2protocol

To define the VPLS pseudowire that is used to transport bridge protocol data unit (BPDU) information between two network provider edge (N-PE) routers, use the **forward permit l2protocol** command in Layer 2 VFI configuration mode. To remove the pseudowire, use the **no** form of this command.

forward permit l2protocol all

no forward permit l2protocol all

Syntax Description

all	Enables the transport of BPDU information between the two N-PE routers.

Command Default

The VPLS pseudowire between the two N-PE routers is not created.

Command Modes

Layer 2 VFI configuration (config-vfi)#

Command History

Release	Modification
12.2(33)SRC	This command was introduced as part of the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature.

Usage Guidelines

Only one pseudowire between the two N-PE routers is allowed.

Examples

The following example creates a VPLS pseudowire between the two N-PE routers:

```
l2 vfi lab2 manual
vpn id 20
forward permit l2protocol all
neigbor 10.10.10.10 encapsulation mpls
```

Related Commands

Command	Description
show vfi	Displays information related to the VFI.

import map

To configure an import route map for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **import map** command in VRF configuration submode.

import map *route-map*

Syntax Description

route-map	Specifies the route map to be used as an import route map for the VRF.

Defaults

A VRF has no import route map unless one is configured using the **import map** command.

Command Modes

VRF configuration submode

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use an import route map when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities configured for the importing and exporting VRF.

The **import map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route. The route map might deny access to selected routes from a community that is on the import list.

The **import map** command does not replace the need for a route-target import in the VRF configuration. You use the **import map** command to further filter prefixes that match a route-target import statement in that VRF.

Examples

The following example shows how to configure an import route map for a VRF:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# import map importmap1
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

index

To insert or modify a path entry at a specific index, use the **index** command in IP explicit path configuration mode. To remove the path entry at the specified index, use the **no** form of this command.

index *index command*

no index *index*

Syntax Description

index	Index number at which the path entry will be inserted or modified. Valid values are from 0 to 65534.
command	An IP explicit path configuration command that creates or modifies a path entry. (You can use only the **next-address** command.)

Defaults

This command is disabled.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to insert the next address at index 6:

```
Router(cfg-ip-expl-path)# index 6 next-address 10.3.29.3

Explicit Path identifier 6:
    6: next-address 10.3.29.3
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
interface fastethernet	Enters the command mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

inter-as-hybrid

To specify a VRF as an Option AB VRF, use the **inter-as-hybrid** command. Routes imported to this VRF can be advertised to Option AB peers and VPNv4 iBGP peers. When routes are received from Option AB peers and imported into the VRF, the next-hop tableid of the route is set to the tableid of the VRF.

inter-as-hybrid [**csc**] [**next-hop** *ip-address*]

no inter-as-hybrid [**csc**] [**next-hop** *ip-address*]

Syntax Description

csc	(Optional) If the **csc** keyword is used, then a per-prefix label is allocated for imported routes. For routes received from Option AB peers that are imported into the VRF, the learned outlabel is installed in forwarding.
next-hop	(Optional) Specifies the next-hop IP address to be set on paths that are imported into the VRF and that are received from an Option AB peer. The next-hop context is also set to the VRF, which imports these paths. If the **next-hop** keyword is not used, the received next-hop is retained but the next-hop context (for paths received from Option AB peers) is still set to that of the VRF.
ip-address	Specifies the IP address of the Inter-AS AB neighbor.

Defaults

No VRF is specified as an Option AB VRF.

Command Modes

VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was modified. It was integrated into the release.

Usage Guidelines

The following usage guidelines apply to the **csc** keyword:

- If the **csc** keyword is not used, a per-VRF label is allocated for imported routes.
- When routes are received from Option AB peers and are imported next into the VRF, the learned out label can only be installed in forwarding when the **csc** keyword is used.
- For routes received from Option AB peers that are imported into the VRF, the learned outlabel is installed in forwarding.

Examples

The following example specifies a VRF as an Option AB VRF:

```
Router(config-vrf-af)# inter-as-hybrid
```

Related Commands

Command	Description
address-family ipv4	Enters VRF address family configuration mode to specify an address family for a VRF.
bgp neighbor inter-as-hybrid	Configures the eBGP peer router (ASBR) as an Inter-AS Option AB peer.
rd	Creates routing and forwarding tables for a VPN.
route-target	Creates a route-target extended community for a VRF.
vrf definition	Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode.

interface auto-template

To create the template interface, use the **interface auto-template** command in global configuration mode. To delete this interface, use the **no** form of this command.

interface auto-template *interface-num*

no interface auto-template

Syntax Description

interface-num	Interface number. Valid values are from 1 to 25.

Command Default

No default behavior or values are required to create templates.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The space before the *interface-num* argument is optional.

Use the **shutdown** command to disable mesh tunnel interface creation when creating a template.

Examples

The following example shows how to create template interface 1:

```
Router(config)# interface auto-template 1
```

Related Commands

Command	Description
clear mpls traffic-eng auto-tunnel mesh	Removes all the mesh tunnel interfaces and re-creates them.
mpls traffic-eng auto-tunnel mesh	Enables autotunnel mesh groups globally.
show mpls traffic-eng auto-tunnel mesh	Displays the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers.

interface xtagatm

Note Effective with Cisco IOS Release 12.4(20)T, the **interface xtagatm** command is not available in Cisco IOS software.

To create an extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface, use the **interface xtagatm** command in global configuration mode.

interface xtagatm *interface-number*

Syntax Description

interface-number	The interface number.

Defaults

XTagATM interfaces are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology.
12.4(20)T	This command was removed.

Usage Guidelines

XTagATM interfaces are virtual interfaces that are created on reference-like tunnel interfaces. An XTagATM interface is created the first time the **interface xtagatm** command is issued for a particular interface number. These interfaces are similar to ATM interfaces, except that the former only supports LC-ATM encapsulation.

Examples

The following example shows how to create an XTagATM interface with interface number 62:

```
Router(config)# interface xtagatm62
```

Related Commands

Command	Description
extended-port	Associates the currently selected extended XTagATM interface with a remotely controlled switch.

interworking

To enable the L2VPN Interworking feature, use the **interworking** command in pseudowire class configuration mode. To disable the L2VPN Interworking feature, use the **no** form of this command.

interworking {**ethernet** | **ip** | **vlan**}

no interworking {**ethernet** | **ip** | **vlan**}

Syntax Description

ethernet	Causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, which leaves a pure Ethernet frame.
ip	Causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. Attachment circuit frames that do not contain IPv4 packets are dropped.
vlan	Causes Ethernet frames and the VLAN tag to be sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped.

Defaults

L2VPN interworking is not enabled.

Command Modes

Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(52)SE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
12.2(33)SRE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.

Usage Guidelines

Table 10 shows which L2VPN Interworking features support Ethernet, IP, and VLAN types of interworking.

Table 10 L2VPN Interworking Feature Support

L2VPN Interworking Feature	Interworking Support
Frame Relay to PPP	IP
Frame Relay to ATM AAL5	IP
Ethernet/VLAN to ATM AAL5	IP and Ethernet
Ethernet/VLAN to Frame Relay	IP and Ethernet
Ethernet/VLAN to PPP	IP
Ethernet to VLAN	IP, Ethernet, and VLAN
L2VPN Interworking: VLAN Enable/Disable Option for AToM	Ethernet VLAN

Examples

The following example shows a pseudowire class configuration that enables the L2VPN Interworking feature:

```
pseudowire-class ip-interworking
 encapsulation mpls
 interworking ip
```

Related Commands

Command	Description
encapsulation l2tpv3	Specifies that L2TPv3 is used as the data encapsulation method for tunneling IP traffic over the pseudowire.
encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.

ip explicit-path

To enter the command mode for IP explicit paths and create or modify the specified path, use the **ip explicit-path** command in global configuration mode. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. To disable this feature, use the **no** form of this command.

ip explicit-path {**name** *word* | **identifier** *number*} [**enable** | **disable**]

no explicit-path {**name** *word* | **identifier** *number*}

Syntax Description

name *word*	Name of the explicit path.
identifier *number*	Number of the explicit path. Valid values are from 1 to 65535.
enable	(Optional) Enables the path.
disable	(Optional) Prevents the path from being used for routing while it is being configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enter the explicit path command mode for IP explicit paths and creates a path numbered 500:

```
Router(config)# ip explicit-path identifier 500
Router(config-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
index	Inserts or modifies a path entry at a specific index.
ip route vrf	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

ip flow-cache mpls label-positions

To enable Multiprotocol Label Switching (MPLS)-Aware NetFlow, use the **ip flow-cache mpls label-positions** command in global configuration mode. To disable MPLS-aware NetFlow, use the **no** form of this command.

ip flow-cache mpls label-positions [*label-position-1* [*label-position-2* [*label-position-3*]]] [**exp-bgp-prefix-fields**] [**no-ip-fields**] [**mpls-length**]

no ip flow-cache mpls label-positions

Syntax Description

label-position-l	(Optional) Position of an MPLS label in the incoming label stack. Label positions are counted from the top of the stack, starting with 1.
exp-bgp-prefix-fields	(Optional) Generates a MPLS Provider Edge (PE) PE-to-PE traffic matrix. The following IP-related flow fields are included: • Input interface • BGP Nexthop • MPLS Experimental (EXP) bits The MPLS label values will be set to zero on the Cisco 10000 in the display output of the **show ip cache verbose flow aggregation exp-bgp-prefix** command.
no-ip-fields	(Optional) Controls the capture and reporting of MPLS flow fields. If the **no-ip-fields** keyword is not specified, the following IP-related flow fields are included: • Source IP address • Destination IP address • Transport layer protocol • Source application port number • Destination application port number • IP type of service (ToS) • TCP flag If the **no-ip-fields** keyword is specified, the IP-related fields are reported with a value of 0.
mpls-length	(Optional) Controls the reporting of packet length. If the **mpls-length** keyword is specified, the reported length represents the sum of the MPLS packet payload length and the MPLS label stack length. If the **mpls-length** keyword is not specified, only the length of the MPLS packet payload is reported.

Defaults

MPLS-Aware NetFlow is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The **no-ip-fields** and **mpls-length** keywords were.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix-fields** keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Use this command to configure the MPLS-aware NetFlow feature on a label switch router (LSR) and to specify labels of interest in the incoming label stack. Label positions are counted from the top of the stack, starting with 1. The position of the top label is 1, the position of the second label is 2, and so forth.

With MPLS-aware NetFlow enabled on the router, NetFlow collects data for incoming IP packets and for incoming MPLS packets on all interfaces where NetFlow is enabled in full or in sampled mode.

Caution When you enter the **ip flow-cache mpls label-positions** command on a Cisco 12000 series Internet router, NetFlow will stop collecting data for incoming IP packets on any Engine 4P line cards installed in the router on which NetFlow is enabled in full or in sampled mode. Engine 4P line cards in a Cisco 12000 series Internet router do not support NetFlow data collection of incoming IP packets and MPLS packets concurrently.

Tip MPLS-aware NetFlow is enabled in global configuration mode. NetFlow is enabled per interface.

Examples

The following example shows how to configure MPLS-aware NetFlow to capture the first (top), third, and fifth label:

```
Router(config)# ip flow-cache mpls label-positions 1 3 5
```

The following example shows how to configure MPLS-aware NetFlow to capture only MPLS flow information (no IP-related flow fields) and the length that represents the sum of the MPLS packet payload length and the MPLS label stack length:

```
Router(config)# ip flow-cache mpls label-positions no-ip-fields mpls-length
```

The following example shows how to configure MPLS PE-to-PE Traffic Statistics for Netflow:

```
Router(config)# ip flow-cache mpls label-positions 1 2 exp-bgp-prefix-fields
```

Related Commands

Command	Description
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.

Command	Description
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip multicast mpls traffic-eng

To enable IP multicast traffic on a tailend router enabled with Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) functionality, use the **ip multicast mpls traffic-eng** command in privileged EXEC mode. To disable IP multicast for MPLS TE P2MP on tailend routers, use the **no** form of this command.

ip multicast mpls traffic-eng [**range** {*access-list-number* | *access-list-name*}]

no ip multicast mpls traffic-eng [**range**]

Syntax Description

range	(Optional) Enables multicast for a specific set of multicast streams.
access-list-number	The specific number of the access list. Valid values are 100–199.
access-list-name	The specific name of the access list.

Command Default

MPLS TE P2MP functionality is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

You configure this command on the tailend routers in an MPLS TE P2MP topology.

Examples

The following example enables multicast routing on tailend routers configured with MPLS TE P2MP functionality:

```
Router(config)# ip multicast-routing
Router(config)# ip multicast mpls traffic-eng
```

Related Commands

Command	Description
show ip mroute	Displays IP multicast forwarding on MPLS TE P2MP tailend routers.

ip path-option

To specify an explicit or dynamic path option for a particular destination address in a destination list, use the **ip path-option** command in traffic engineering destination list configuration mode. To remove the path option, use the **no** form of this command.

ip *ip-address* **path-option** *id* {**dynamic** | **explicit** {**name** *name* | **identifier** *number*} [**verbatim**]}

no ip *ip-address* **path-option** *id*

Syntax Description

ip-address	The destination address of the path.
id	The preference for this path option for the same destination address. The valid values are 1–1000. Only one path option is supported for each destination address.
dynamic	Specifies that the traffic engineering paths be dynamically computed.
explicit	Specifies that the traffic engineering paths be explicitly configured.
name *name*	Specifies the name of the explicit path.
identifier *number*	Specifies the number of the explicit path.
verbatim	(Optional) Specifies that the path should be sent out without any checking.

Command Default

Path options are not configured.

Command Modes

Traffic engineering destination list (cfg-te-dest-list)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

- The **ip path-option** command is supported at a sublabel switched path (sub-LSP) level.
- Point-to-multipoint traffic engineering supports only one path option per destination.

Examples

The following example shows the configuration of a destination list with explicit path options:

```
Router(config)# mpls traffic-eng destination list identifier 1
Router(cfg-te-dest-list)# ip 10.10.10.10 path-option 1 explicit identifier 1
```

Related Commands

Command	Description
mpls traffic-eng destination list	Specifies a MPLS traffic engineering point-to-multipoint destination list.

ip route static inter-vrf

To allow static routes to point to Virtual Private Network (VPN) routing and forwarding (VRF) interfaces other than those to which the static route belongs, use the **ip route static inter-vrf** command in global configuration mode. To prevent static routes from pointing to VRF interfaces in VRFs to which they do not belong, use the **no** form of this command.

ip route static inter-vrf

no ip route static inter-vrf

Syntax Description

This command has no arguments or keywords.

Defaults

Static routes are allowed to point to VRF interfaces in any VRF.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip route static inter-vrf** command is turned on by default. The **no ip route static inter-vrf** command causes the respective routing table (global or VRF) to reject the installation of static routes if the outgoing interface belongs to a different VRF than the static route being configured. This prevents security problems that can occur when static routes that point to a VRF interface in a different VRF are misconfigured. You are notified when a static route is rejected, then you can reconfigure it.

For example, a static route is defined on a provider edge (PE) router to forward Internet traffic to a customer on the interface pos1/0, as follows:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 1/0
```

The same route is mistakenly configured with the next hop as the VRF interface pos10/0:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 10/0
```

By default, Cisco IOS software accepts the command and starts forwarding the traffic to both pos1/0 (Internet) and pos10/0 (VPN) interfaces.

If the static route is already configured that points to a VRF other than the one to which the route belongs when you issue the **no ip route static inter-vrf** command, the offending route is uninstalled from the routing table and a message similar to the following is sent to the console:

```
01:00:06: %IPRT-3-STATICROUTESACROSSVRF: Un-installing static route x.x.x.x/32 from global
routing table with outgoing interface intx/x
```

If you enter the **no ip route static inter-vrf** command before a static route is configured that points to a VRF interface in a different VRF, the static route is not installed in the routing table and a message is sent to the console.

Configuring the **no ip route static inter-vrf** command prevents traffic from following an unwanted path. A VRF static route points to a global interface or any other VRF interface as shown in the following **ip route vrf** commands:

- Interface serial 1/0.0 is a global interface:

```
Router(config)# no ip route static inter-vrf

Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 serial 1/0.0
```

- Interface serial 1/0.1 is in vpn2:

```
Router(config)# no ip route static inter-vrf

Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 serial 1/0.1
```

With the **no ip route static inter-vrf** command configured, these static routes are not installed into the vpn1 routing table because the static routes point to an interface that is not in the same VRF.

If you require a VRF static route to point to a global interface, you can use the **global** keyword with the **ip route vrf** command:

```
Router(config)# ip route vrf vpn1 10.12.1.1 255.255.255.255 serial 1/0.0 10.0.0.1 global
```

The **global** keyword allows the VRF static route to point to a global interface even when the **no ip route static inter-vrf** command is configured.

Examples

The following example shows how to prevent static routes that point to VRF interfaces in a different VRF:

```
Router(config)# no ip route static inter-vrf
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.

ip route vrf

To establish static routes for a Virtual private Network (VPN) routing and forwarding (VRF) instance, use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

no ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.
next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Type of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
global	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
distance	(Optional) An administrative distance for this route.
permanent	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Label (tag) value that can be used for controlling redistribution of routes through route maps.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use a static route when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through the Routing Information Protocol (RIP), IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface not defined in a network command, no dynamic routing protocols advertise the route unless a **redistribute static** command is specified for these protocols.

Supported Static Route Configurations

When configuring static routes in a Multiprotocol Label Switching (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 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 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 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 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 equipment (CE) side. For example, the following command is supported when the destination prefix is the CE router's loopback address, as in external BGP (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**

Examples

The following command shows how to reroute packets addressed to network 10.23.0.0 in VRF vpn3 to router 10.31.6.6:

```
Router(config)# ip route vrf vpn3 10.23.0.0 255.255.0.0 10.31.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.

ip rsvp msg-pacing

To set up message pacing (that is, to control the transmission rate for Resource Reservation Protocol (RSVP) messages), use the **ip rsvp msg-pacing** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp msg-pacing [**period** *ms* [**burst** *msgs* [**maxsize** *qsize*]]]

no rsvp msg-pacing

Syntax Description

period *ms*	(Optional) Length of the interval, in milliseconds, during which a router can send the number of RSVP messages specified in the *burst* keyword. The value can be from 1 to 1000 milliseconds.
burst *msgs*	(Optional) Maximum number of RSVP messages that a router can send to an output interface during each interval specified in the *period* keyword. The value can be from 1 to 2000.
maxsize *qsize*	(Optional) Size of per-interface output queues in the sending router. Valid values are from 1 to 2000.

Command Default

RSVP messages are not paced.
If you enter the command without the optional arguments, the transmission rate for RSVP messages is limited to 200 messages per second per outgoing interface.
The default output queue size, specified in the **maxsize** keyword, is 500.

Command Modes

Global configuration

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use this command to prevent a burst of RSVP traffic engineering signaling messages from overflowing the input queue of a receiving router, which would cause the router to drop some messages. Dropped messages substantially delay the completion of signaling for LSPs for which messages have been dropped.

Examples

In the following example, a router can send a maximum of 150 RSVP traffic engineering signaling messages in 1 second to a neighbor, and the size of the output queue is 750:

```
Router(config)# ip rsvp msg-pacing period 1 burst 150 maxsize 750
```

Related Commands

Command	Description
clear ip rsvp msg-pacing	Clears the RSVP message pacing output from the **show ip rsvp neighbor** command.

ip rsvp signalling hello (configuration)

To enable Hello globally on the router, use the **ip rsvp signalling hello** command in global configuration mode. To disable Hello globally on the router, use the **no** form of this command.

ip rsvp signalling hello

no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

To enable Hello globally on the router, you must enter this command. You also must enable Hello on the interface.

Examples

In the following example, Hello is enabled globally on the router:

```
Router(config)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

ip rsvp signalling hello (interface)

To enable Hello on an interface where you need Fast Reroute protection, use the **ip rsvp signalling hello** command in interface configuration mode. To disable Hello on an interface where you need Fast Reroute protection, use the **no** form of this command

ip rsvp signalling hello

no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

You must configure Hello globally on the router and on the specific interface.

Examples

In the following example, Hello is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the Hello messages sent out from the interface.
ip rsvp signalling hello refresh misses	Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.

ip rsvp signalling hello bfd (configuration)

To enable the Bidirectional Forwarding Detection (BFD) protocol globally on the router for Multiprotocol Label Switching (MPLS) traffic engineering (TE) link and node protection, use the **ip rsvp signalling hello bfd** command in global configuration mode. To disable BFD globally on the router, use the **no** form of this command.

ip rsvp signalling hello bfd

no ip rsvp signalling hello bfd

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled globally on the router for MPLS TE link and node protection.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

To enable the BFD protocol on the router, you must enter this command. You also must enter the **ip rsvp signalling hello bfd** command on the interface.

Examples

The following example allows you to use the BFD protocol on the router for MPLS TE link and node protection:

```
Router(config)# ip rsvp signalling hello bfd
```

Related Commands

Command	Description
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol on an interface where you need MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

ip rsvp signalling hello bfd (interface)

To enable the Bidirectional Forwarding Detection (BFD) protocol on an interface for Multiprotocol Label Switching (MPLS) traffic engineering (TE) link and node protection, use the **ip rsvp signalling hello bfd** command in interface configuration mode. To disable BFD on an interface for MPLS TE link and node protection, use the **no** form of this command.

ip rsvp signalling hello bfd

no ip rsvp signalling hello bfd

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

You must enter the **ip rsvp signalling hello bfd** command on the router and on the specific interface.

Examples

In the following example, the BFD protocol is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello bfd
```

Related Commands

Command	Description
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol on the router for MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

ip rsvp signalling hello dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) hello message sent from an interface, use the **ip rsvp signalling hello dscp** command in interface configuration mode. To set the DSCP value to its default, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **dscp** *num*

no ip rsvp signalling hello [**fast-reroute**] **dscp**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
num	DSCP value. Valid values are from 0 to 63.

Command Default

The default DSCP value is 48.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

If a link is congested, it is recommended that you set the DSCP to a value higher than 0 to reduce the likelihood that hello messages will be dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to the RSVP hellos created on a specific interface. You can configure each interface independently for DSCP.

If you issue the **ip rsvp signalling hello dscp** command without the optional **fast-reroute** keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **ip rsvp signalling hello fast-reroute dscp** command.

Examples

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute dscp 30
```

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello dscp 30
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables hellos on an interface where you need Fast Reroute protection.
ip rsvp signalling hello refresh interval	Sets the hello refresh interval in hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) hello refresh interval, use the **ip rsvp signalling hello refresh interval** command in interface configuration mode. To set the refresh interval to its default value, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh interval** *interval-value*

no ip rsvp signalling hello [**fast-reroute**] **refresh interval**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
interval-value	Frequency, in milliseconds (msec), at which a node sends hello messages to a neighbor. Valid values are from 10 to 30000 msec. **Note** Values below the default of 200 msec are not recommended, because they can cause RSVP Hellos to falsely detect a neighbor down event and unecessarily trigger Fast ReRoute.

Command Default

The default frequency at which a node sends hello messages to a neighbor is 200 msec.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can configure the hello request interval on a per-interface basis. A node periodically generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the hello interval.

If you issue the **ip rsvp signalling hello refresh interval** command without the optional **fast-reroute** keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **ip rsvp signalling hello fast-reroute refresh interval** command.

Examples

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh interval 5000
```

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh interval 5000
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello graceful-restart fresh interval	Sets the refresh interval in graceful restart hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello refresh misses

To specify how many Resource Reservation Protocol (RSVP) traffic engineering (TE) hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down, use the **ip rsvp signalling hello refresh misses** command in interface configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh misses** *msg-count*

no ip rsvp signalling hello [**fast-reroute**] **refresh misses**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
msg-count	Number of sequential hello acknowledgments that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10.

Command Default

The default *number of sequential hello acknowledgments* is 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

A hello comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is very congested or a router has a very heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

If you issue the **ip rsvp signalling hello refresh misses** command without the optional **fast-reroute** keyword, the command applies to Fast Reroute hellos and Fast Reroute capability is enabled by default. This command is provided for backward compatibility; however, we recommend that you use the **ip rsvp signalling hello fast-reroute refresh misses** command.

Examples

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh misses 5
```

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh misses 5
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello refresh interval	Sets the refresh interval in hello messages.

ip rsvp signalling hello statistics

To enable Hello statistics on the router, use the **ip rsvp signalling hello statistics** command in global configuration mode. To disable Hello statistics on the router, use the **no** form of this command.

ip rsvp signalling hello statistics

no ip rsvp signalling hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

In the following example, Hello statistics are enabled on the router.

```
Router(config)# ip rsvp signalling hello statistics
```

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
ip vrf vpn1
 rd 100:2
 route-target both 100:2
 route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (**interface configuration**)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf forwarding (interface configuration)

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with an interface or subinterface, use the **ip vrf forwarding** command in interface configuration mode. To disassociate a VRF, use the **no** form of this command.

ip vrf forwarding *vrf-name* [**downstream** *vrf-name2*]

no ip vrf forwarding *vrf-name* [**downstream** *vrf-name2*]

Syntax Description

vrf-name	Associates the interface with the specified VRF.
downstream	(Optional) Enables Half Duplex VRF (HDVRF) functionality on the interface and associates the interface with the downstream VRF.
vrf-name2	(Optional) Associates the interface with the specified downstream VRF.

Defaults

The default for an interface is the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(6)	The **downstream** keyword was added to support MPLS VPN Half-Duplex VRFs.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use this command to associate an interface with a VRF. Executing this command on an interface removes the IP address. The IP address should be reconfigured. The **downstream** keyword is available on supported platforms with virtual interfaces. The **downstream** keyword associates the interfaces with a downstream VRF, which enables half duplex VRF functionality on the interface. Some functions operate in the upstream VRFs, and others operate in the downstream VRFs. The following functions operate in the downstream VRFs:

- PPP peer routes are installed in the downstream VRFs.
- Authentication, authorization, and accounting (AAA) per-user routes are installed in the downstream VRFs.

- A Reverse Path Forwarding (RPF) check is performed in the downstream VRFs.

Examples

The following example shows how to link a VRF to ATM interface 0/0:

```
Router(config)# interface atm0/0
Router(config-if)# ip vrf forwarding vpn1
```

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
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.
ip vrf	Configures a VRF routing table.

ip vrf receive

To insert the IP address of an interface as a connected route entry in a Virtual Private Network (VPN) routing and forwarding instance (VRF) routing table, use the **ip vrf receive** command in interface configuration mode. To remove the connected entry from the VRF routing table, use the **no** form of this command.

ip vrf receive *vrf-name*

no ip vrf receive *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF into which you want to add the IP address of the interface.

Command Default

No IP address of an interface is inserted as connected route entry in a VRF routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip vrf receive** command supports VRF route selection for the following features:

- MPLS VPN: VRF Selection Based on Source IP Address
- MPLS VPN: VRF Selection Using Policy-Based Routing

This command is used to install a primary or secondary IP address of an interface as a connected route entry in the VRF routing table. These entries appear as “receive” entries in the Cisco Express Forwarding table. MPLS VPNs require Cisco Express Forwarding switching to make IP destination prefix-based switching decisions. This command can be used to selectively install the interface IP address in the VRF that is specified with the *vrf-name* argument. Only the local interface IP address is added to the VRF routing table. This command is used on a per-VRF basis. In other words, you must enter this command for each VRF in which you need to insert the IP address of the interface. This command does not remove the interface IP address from the global routing table.

Note This command cannot be used with the **ip vrf forward** command for the same interface.

VRF Selection Based on Source IP Address Guidelines

The **ip vrf receive** command is automatically disabled when the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the **ip vrf receive** command is disabled in this manner. Interfaces where the VRF Selection Based on Source IP Address feature is enabled can forward packets that have an IP address that corresponds to an IP address entry in the VRF table. If the VRF table does not contain a matching IP address, the packet is dropped, by default, because there is no corresponding “receive” entry in the VRF entry.

VRF Selection Using Policy Based Routing Guidelines

You must enter the **ip policy route-map** command before the **ip vrf receive** command can be enabled. The **ip vrf receive** command is automatically disabled when either the **no ip policy route-map** *map-name* or the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the **ip vrf receive** command is disabled in this manner. With the VRF Selection Using Policy-Based Routing implementation of the VRF selection feature, a route map filters the VRF routes. If a match and set operation occurs in the route map but there is no receive entry in the local VRF table, the packet is dropped.

Examples

VRF Selection Based on Source IP Address

The following example shows how to configure Ethernet interface 0/2 (172.16.1.3) and insert its IP address in VRF1 and VRF2 with the **ip vrf receive** command. You must enter the **ip vrf select source** command on the interface or subinterface to enable VRF selection on the interface or subinterface. You must also enter the **vrf selection source** command in global configuration mode to populate the VRF selection table and to configure the VRF Selection Based on Source IP Address feature. (The **vrf selection source** command is not shown in this example.)

```
Router(config)# interface Ethernet0/2
Router(config-if)# ip address 172.16.1.3 255.255.255.255
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf receive VRF1
Router(config-if)# ip vrf receive VRF2
Router(config-if)# end
```

VRF Selection Using Policy-Based Routing

The following example shows how to configure Ethernet interface 0/1 (192.168.1.2) and insert its IP address in VRF1 and VRF2 with the **ip vrf receive** command. You must configure an access list and a route map to allow the VRF Section Using Policy-Based Routing feature to select a VRF. (The access list and route map configuration are not shown in this example.)

```
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 192.168.1.2 255.255.255.255
Router(config-if)# ip policy route-map PBR-VRF-SELECTION
Router(config-if)# ip vrf receive VRF1
Router(config-if)# ip vrf receive VRF2
Router(config-if)# end
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip vrf	Configures a VRF routing table.
ip vrf select source	Enables VRF selection on an interface.
set vrf	Enables VRF selection and filtering under a route map.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF selection table.

ip vrf select source

To enable the VRF Selection feature on a particular interface or subinterface, use the **ip vrf select source** command in interface configuration mode. To disable the VRF Selection feature on a particular interface or subinterface, use the **no** form of this command.

ip vrf select source

no ip vrf select source

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip vrf select source** and **ip vrf forwarding** commands are mutually exclusive. If the VRF Selection feature is configured on an interface, you cannot configure VRFs (using the **ip vrf forwarding** command) on the same interface.

Examples

The following example shows how to enable the VRF Selection feature on an interface:

```
Router(config-if)# ip vrf select source
```

The following example shows the message you receive after you have deleted the VRF Selection feature on an interface:

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# interface pos4/0
Router (config-if)# no ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT unset for POS4/0, slot: 4
Router (config-if)#
```

The following example shows the message you receive after you have enabled the VRF Selection feature on an interface:

```
Router (config-if)#
Router (config-if)# ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT set for POS4/0, slot: 4
Router (config-if)#
```

Related Commands

Command	Description
ip vrf receive	Adds all the IP addresses that are associated with an interface into a VRF table.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF Selection table.

ip vrf sitemap

To configure Site of Origin (SoO) filtering on an interface, use the **ip vrf sitemap** command in interface configuration mode. To disable SoO filtering on an interface, use the **no** form of this command.

ip vrf sitemap *route-map*

no ip vrf sitemap

Syntax Description

route-map	The name of the route map that is configured with the as-number and network of the VPN site.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community attribute uniquely identifies the site from which a PE router has learned a route.

Examples

The following example configures SoO filtering on an interface:

```
Router(config)# route-map Site-of-Origin permit 10
Router(config-route-map)# set extcommunity soo 100:1
Router(config-route-map)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip vrf forwarding RED
Router(config-if)# ip vrf sitemap Site-of-Origin
Router(config-if)# ip address 10.0.0.1 255.255.255.255
Router(config-if)# end
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

l2 vfi point-to-point

To establish a point-to-point Layer 2 virtual forwarding interface (VFI) between two separate networks, use the **l2 vfi point-to-point** command in global configuration mode. To disable the connection, use the **no** form of this command.

l2 vfi *name* **point-to-point**

no l2 vfi *name* **point-to-point**

Syntax Description

name	Name of the connection between the two networks.

Command Default

Point-to-point Layer 2 virtual forwarding interfaces are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If you disable L2VPN Pseudowire Switching with the **no l2 vfi point-to-point** command, the virtual circuits (VCs) are deleted.

Examples

The following example establishes a point-to-point Layer 2 VFI:

```
Router(config)# l2 vfi atomvfi point-to-point
```

Related Commands

Command	Description
neighbor (L2VPN Pseudowire Switching)	Establishes the two routers with which to form a connection.

list

To show all or part of the explicit path or paths, use the **list** command in IP explicit path configuration mode.

list [*starting-index-number*]

Syntax Description

starting-index-number	(Optional) Index number at which the explicit path(s) will start to be displayed. Valid values are from 1 to 65535.

Defaults

Explicit paths are not shown.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to list the explicit path:

```
Router(cfg-ip-expl-path)# list

Explicit Path name path1:
    1:next-address 10.0.0.1
    2:next-address 10.0.0.2
```

The following example shows how to list the explicit path starting at index number 2:

```
Router(cfg-ip-expl-path)# list 2

Explicit Path name path1:
    2:next-address 10.0.0.2
Router(cfg-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
index	Inserts or modifies a path entry at a specific index.
ip explicit-path	Enters the command mode for IP explicit paths, and creates or modifies the specified path.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

list (LSP Attributes)

To display the contents of a label switched path (LSP) attribute list, use the **list** command in LSP Attributes configuration mode.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Contents of an LSP attribute list is not displayed.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command displays the contents of the LSP attribute list. You can display each of the following configurable LSP attributes using the **list** command: affinity, auto-bw, bandwidth, lockdown, priority, protection, and record-route.

Examples

The following example shows how to display the contents of an LSP attribute list identified with the string priority:

```
!
Router(config)# mpls traffic-eng lsp attributes priority
Router(config-lps-attr)# priority 0 0
Router(config-lps-attr)# list

LIST priority
 priority 0 0

Router(config-lsp-attr)#
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

lockdown (LSP Attributes)

To disable reoptimization of the label switched path (LSP), use the **lockdown** command in LSP Attributes configuration mode. To reenable reoptimization, use the **no** form of this command.

lockdown

no lockdown

Syntax Description

This command has no arguments or keywords.

Command Default

Reoptimization of the LSP is enabled.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up in an LSP attribute list the disabling of reoptimization of an LSP triggered by a timer, or the issuance of the **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of an LSP.

To associate the LSP lockdown attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to configure disabling of reoptimization in an LSP attribute list:

```
Configure terminal
!
mpls traffic-eng lsp attributes 4
 bandwidth 1000
 priority 1 1
 lockdown
 end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

match mpls-label

To redistribute routes that include Multiprotocol Label Switching (MPLS) labels if the routes meet the conditions specified in the route map, use the **match mpls-label** command in route-map configuration mode. To disable this function, use the **no** form of this command.

match mpls-label

no match mpls-label

Syntax Description

This command has no arguments or keywords.

Command Default

Routes with MPLS labels are not redistributed.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A route map that includes this command can be used in the following instances:

- With the **neighbor route-map in** command to manage inbound route maps in BGP
- With the **redistribute bgp** command to redistribute route maps in an IGP

Use the **route-map** global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match route-map** configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

The following example shows how to create a route map that redistributes routes if the following conditions are met:

- The IP address of the route matches an IP address in access control list 2.
- The route includes an MPLS label.

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 2
Router(config-route-map)# match mpls-label
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set mpls-label	Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.

maximum routes

To limit the maximum number of routes in a Virtual Private Network (VPN) routing and forwarding (VRF) instance to prevent a provider edge (PE) router from importing too many routes, use the **maximum routes** command in VRF configuration mode or VRF address family configuration mode. To remove the limit on the maximum number of routes allowed, use the **no** form of this command.

maximum routes *limit* {*warn-threshold* | **warning-only**}

no maximum routes

Syntax Description

limit	The maximum number of routes allowed in a VRF. The valid range is from 1 to 4294967295 routes.
warn-threshold	The warning threshold value expressed as a percentage (from 1 to 100) of the *limit* value. When the number of routes reaches the specified percentage of the limit, a warning message is generated.
warning-only	Issues a system message logging (syslog) error message when the maximum number of routes allowed for a VRF exceeds the threshold. However, additional routes are still allowed.

Command Default

No limit is set on the maximum number of routes allowed.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(13)T	Support for Simple Network Management Protocol (SNMP) notifications was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	Support for this command was added for IPv6 address families under the **vrf definition** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **maximum routes** command can be configured in one of two ways:

- Generate a warning message when the *limit* value is exceeded
- Generate a warning message when the *warn-threshold* value is reached

To limit the number of routes allowed in the VRF, use the **maximum routes** *limit* command with the *warn-threshold* argument. The *warn-threshold* argument generates a warning and does not allow the addition of routes to the VRF when the maximum number set by the *limit* argument is reached. The software generates a warning message every time a route is added to a VRF when the VRF route count is above the warning threshold. The software also generates a route rejection notification when the maximum threshold is reached and every time a route is rejected after the limit is reached.

To set a number of routes at which you receive a notification, but which does not limit the number of routes that can be imported into the VRF, use the **maximum routes** *limit* command with the **warn-only** keyword.

To configure the router to generate SNMP notifications (traps or informs) for these values, use the **snmp-server enable traps mpls vpn** command in global configuration mode.

Examples

The following example shows how to set a limit threshold of VRF routes to 1000. When the number of routes for the VRF reaches 1000, the router issues a syslog error message, but continues to accept new VRF routes.

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# maximum routes 1000 warning-only
```

The following example shows how to set the maximum number of VRF routes allowed to 1000 and set the warning threshold at 80 percent of the maximum. When the number of routes for the VRF reaches 800, the router issues a warning message. When the number of routes for the VRF reaches 1000, the router issues a syslog error message and rejects any new routes.

```
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 200:1
Router(config-vrf)# route-target import 200:1
Router(config-vrf)# maximum routes 1000 80
```

The following example for an IPv6 address family defined under the **vrf definition** command shows how to set the maximum number of VRF routes allowed to 500 and set the warning threshold at 50 percent of the maximum. When the number of routes for the VRF reaches 250, the router issues a warning message. When the number of routes for the VRF reaches 500, the router issues a syslog error message and rejects any new routes.

```
Router(config)# vrf definition
Router(config-vrf)# address-family ipv6
Router(config-router-vrf)# maximum routes 500 50
```

Related Commands

Command	Description
address-family (VRF configuration)	Enters VRF address family configuration mode to select an address family type for a VRF table.
import map	Configures an import route map for a specified VRF for more control over routes imported into the VRF.
ip vrf	Specifies a name for a VRF routing table and enters VRF configuration mode (for IPv4 only).
rd	Creates VRF routing and forwarding tables and specifies the default route distinguisher for a VPN.

Command	Description
route-target	Configures a VRF route target community for importing and exporting extended community attributes.
snmp-server enable traps mpls vpn	Enables the router to send MPLS VPN-specific SNMP notifications (traps and informs).
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

metric-style narrow

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it generates and accepts old-style type, length, and value objects (TLVs), use the **metric-style narrow** command in router configuration mode. To disable this function, use the **no** form of this command.

metric-style narrow [**transition**] [**level-1** | **level-2** | **level-1-2**]

no metric-style narrow [**transition**] [**level-1** | **level-2** | **level-1-2**]

Syntax Description

transition	(Optional) Instructs the router to use both old- and new-style TLVs.
level-1	(Optional) Enables this command on routing level 1.
level-2	(Optional) Enables this command on routing level 2.
level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Defaults

The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure the router to generate and accept old-style TLVs on router level 1:

```
Router(config-router)# metric-style narrow level-1
```

Related Commands

Command	Description
metric-style transition	Configures a router to generate both old-style and new-style TLVs.
metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style transition

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it generates and accepts both old-style and new-style type, length, and value objects (TLVs), use the **metric-style transition** command in router configuration mode. To disable this function, use the **no** form of this command.

metric-style transition [**level-1** | **level-2** | **level-1-2**]

no metric-style transition [**level-1** | **level-2** | **level-1-2**]

Syntax Description

level-1	(Optional) Enables this command on routing level 1.
level-2	(Optional) Enables this command on routing level 2.
level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Defaults

The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure a router to generate and accept both old-style and new-style TLVs on router level 2:

```
Router(config-router)# metric-style transition level-2
```

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept old-style TLVs.
metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style wide

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it generates and accepts only new-style type, length, and value objects (TLVs), use the **metric-style wide** command in router configuration mode. To disable this function, use the **no** form of this command.

metric-style wide [**transition**] [**level-1** | **level-2** | **level-1-2**]

no metric-style wide [**transition**] [**level-1** | **level-2** | **level-1-2**]

Syntax Description

transition	(Optional) Instructs the router to accept both old- and new-style TLVs.
level-1	(Optional) Enables this command on routing level 1.
level-2	(Optional) Enables this command on routing level 2.
level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Defaults

The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you enter the **metric-style wide** command, a router generates and accepts only new-style TLVs. Therefore, the router uses less memory and other resources than it would if it generated both old-style and new-style TLVs.

This style is appropriate for enabling MPLS traffic engineering across an entire network.

Note This discussion of metric styles and transition strategies is oriented toward traffic engineering deployment. Other commands and models could be appropriate if the new-style TLVs are desired for other reasons. For example, a network might require wider metrics, but might not use traffic engineering.

Examples

The following example shows how to configure a router to generate and accept only new-style TLVs on level 1:

```
Router(config-router)# metric-style wide level-1
```

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept old-style TLVs.
metric-style transition	Configures a router to generate and accept both old-style and new-style TLVs.

mls mpls

To enable Multiprotocol Label Switching (MPLS) recirculation, use the **mls mpls** command in global configuration mode. To disable MPLS recirculation, use the **no** form of this command.

mls mpls {**recir-agg** | **tunnel-recir**}

no mls mpls {**recir-agg** | **tunnel-recir**}

Syntax Description

recir-agg	Recirculates the MPLS aggregated-label packets (only new aggregated labels are impacted).
tunnel-recir	Recirculates the tunnel-MPLS packets.

Defaults

MPLS recirculation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17b)SXA	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that have to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Cisco 7600 series router.

Examples

The following example shows how to enable aggregated-label MPLS recirculation:

```
Router(config)# mls mpls recir-agg
```

The following example shows how to enable tunnel-MPLS recirculation:

```
Router(config)# mls mpls tunnel-recir
```

The following example shows how to disable aggregated-label MPLS recirculation:

```
Router(config)# no mls mpls recir-agg
```

The following example shows how to disable tunnel-MPLS recirculation:

```
Router(config)# no mls mpls tunnel-recir
```

mls mpls (guaranteed bandwidth traffic engineering)

To configure the guaranteed bandwidth traffic engineering flow parameters globally, use the **mls mpls** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls mpls {**gb-te-burst** *burst* | **gb-te-cir-ratio** *ratio* | **gb-te-dscp** *dscp-value* [**markdown**] | **gb-te-enable** [**global-pool**]}

no mls mpls {**gb-te-burst** *burst* | **gb-te-cir-ratio** *ratio* | **gb-te-dscp** *dscp-value* [**markdown**] | **gb-te-enable** [**global-pool**]}

Syntax Description

gb-te-burst *burst*	Specifies the burst duration for the guaranteed bandwidth traffic engineering flows; valid values are from 100 to 30000 milliseconds.
gb-te-cir-ratio *ratio*	Specifies the ratio for the committed information rate policing; valid values are from 1 to 100 percent.
gb-te-dscp *dscp-value*	Specifies the differentiated services code point (DSCP) map for the guaranteed bandwidth traffic engineering flows; valid values are from 0 to 63.
markdown	(Optional) Marks down or drops the nonconforming flows.
gb-te-enable	Enables the guaranteed bandwidth traffic engineering flow policing.
global-pool	(Optional) Specifies using resources allocated from the global pool to the police traffic engineering flows.

Defaults

The default settings are as follows:

- *burst* is 1000 milliseconds.
- *ratio* is 1 percent.
- *dscp-value* is 40.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Use the **mls qos map dscp-exp** command to reset the Exp value of the Multiprotocol Label Switching (MPLS) packet when the out-label gets swapped.

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that need to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Cisco 7600 series router.

Use the **show erm statistics** command to display the Forwarding Information Base (FIB) Ternary Content Addressable Memory (TCAM) exception status for IPv4, IPv6, and MPLS protocols.

Examples

This example shows how to specify the burst duration for the guaranteed bandwidth traffic engineering flows:

```
Router(config)# mls mpls gb-te-burst 2000
Router(config)#
```

This example shows how to specify the ratio for CIR policing:

```
Router(config)# mls mpls gb-te-ratio 30
Router(config)#
```

This example shows how to specify the DSCP map for the guaranteed bandwidth traffic engineering flows and to drop the nonconforming flows:

```
Router(config)# mls mpls gb-te-dscp 25 markdown
Router(config)#
```

This example shows how to enable the guaranteed bandwidth traffic engineering flow policing:

```
Router(config)# mls mpls gb-te-enable
Router(config)#
```

Related Commands

Command	Description
show erm statistics	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

mls mpls (recirculation)

To enable Multiprotocol Label Switching (MPLS) recirculation, use the **mls mpls** command in global configuration mode. To disable MPLS recirculation, use the **no** form of this command.

mls mpls {**recir-agg** | **tunnel-recir**}

no mls mpls {**recir-agg** | **tunnel-recir**}

Syntax Description

recir-agg	Recirculates the MPLS aggregated-label packets (new aggregated labels are impacted only).
tunnel-recir	Recirculates the tunnel-MPLS packets.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that need to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Cisco 7600 series router.

Use the **show erm statistics** command to display the Forwarding Information Base (FIB) Ternary Content Addressable Memory (TCAM) exception status for IPv4, IPv6, and MPLS protocols.

Examples

This example shows how to enable the aggregated-label MPLS recirculation:

```
Router(config)# mls mpls recir-agg
Router(config)#
```

This example shows how to enable the tunnel-MPLS recirculation:

```
Router(config)# mls mpls tunnel-recir
Router(config)#
```

This example shows how to disable the aggregated-label MPLS recirculation:

```
Router(config)# no mls mpls recir-agg
Router(config)#
```

This example shows how to disable the tunnel-MPLS recirculation:

```
Router(config)# no mls mpls tunnel-recir
Router(config)#
```

Related Commands

Command	Description
show erm statistics	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

mpls atm control-vc

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm control-vc** command is not available in Cisco IOS software.

To configure the control-VC virtual path identifier (VPI) and virtual circuit identifier (VCI) values for the initial link to the Multiprotocol Label Switching (MPLS) peer, use the **mpls atm control-vc** command in interface configuration mode. To unconfigure the values, use the **no** form of this command.

mpls atm control-vc *vpi vci*

no mpls atm control-vc *vpi vci*

Syntax Description

vpi	Virtual path identifier, in the range from 0 to 4095.
vci	Virtual circuit identifier, in the range from 0 to 65535.

Defaults

0/32

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology. The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

Use this command to establish the LDP session and to carry non-IP traffic. The default VPI VCI for the control VC is (0, 32). If for any reason you need to have a different control-VC, use the **mpls atm control-vc** command to configure any VPI VCI allowed by the *vpi* and *vci* arguments for the control VC.

Examples

The following example shows an MPLS subinterface and VPI 1 and VCI 34 as the control VCs:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm control-vc 1 34
```

Related Commands

Command	Description
mpls ip (interface)	Enables label switching of IPv4 packets on an interface.

mpls atm cos

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm cos** command is not available in Cisco IOS software.

To change the configured bandwidth allocation for class of service (CoS), use the **mpls atm cos** command in global configuration mode.

mpls atm cos {**available** | **standard** | **premium** | **control**} *weight*

Syntax Description

available	The weight for the available class. This is the lowest class priority.
standard	The weight for the standard class. This is the next lowest class priority.
premium	The weight for the premium class. This is the next highest class priority.
control	The weight for the control class. This is the highest class priority.
weight	The total weight for all CoS traffic classes. This value ranges from 0 to 100.

Defaults

Available 50%, control 50%

Command Modes

Global configuration (config)

Command History

Release	Modifications
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology.
12.4(20)T	This command was removed.

Examples

The following example shows how to configure the XTagATM interface for CoS traffic:

```
Router(config)# interface xtagatm12
Router(config-if)# extended-port atm1/0 descriptor 1.2
Router(config-if)# mpls ip
Router(config-if)# mpls atm cos available 49
Router(config-if)# mpls atm cos standard 50
Router(config-if)# mpls atm cos premium 0
Router(config-if)# mpls atm cos control 1
```

mpls atm disable-headend-vc

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm disable-headend-vc** command is not available in Cisco IOS software.

To remove all headend virtual circuits (VCs) from the Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC) and disable its ability to function as an edge label switch router (LSR), use the **mpls atm disable-headend-vc** command in global configuration mode. To restore the headend VCs of the MPLS LSC and restore full edge LSR functionality, use the **no** form of this command.

mpls atm disable-headend-vc

no mpls atm disable-headend-vc

Syntax Description

This command has no arguments or keywords.

Defaults

Edge LSR is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)DC	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology.
12.4(20)T	This command was removed.

Usage Guidelines

This command prevents the LSC from initiating headend label VCs (LVCs), and thus reduces the number of LVCs used in the network.

Examples

The following example shows how to disable the MPLS LSC from acting like an edge LSR and therefore cannot create headend LVCs:

```
mpls atm disable-headend-vc
```

mpls atm multi-vc

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm multi-vc** command is not available in Cisco IOS software.

To configure a router subinterface to create one or more label virtual circuits (VCs) over which packets of different classes are sent, use the **mpls atm multi-vc** command in ATM subinterface submode. To remove the label virtual circuits, use the **no** form of this command.

mpls atm multi-vc

no mpls atm multi-vc

Syntax Description

This command has no arguments or keywords.

Command Modes

ATM subinterface submode (config-subif)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.4(20)T	This command was removed.

Usage Guidelines

This command is valid only on ATM MPLS subinterfaces.

Examples

The following example shows how to configure interface ATM2/0/0.1 on the networking device for MPLS quality of service (QoS) multi-VC mode:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ATM2/0/0.1 mpls
Router(config-subif)# mpls atm multi-vc
Router(config-subif)# exit
Router(config)# exit
```

Related Commands

Command	Description
mpls cos-map	Creates a class map that specifies how classes map to label virtual circuits when they are combined with a prefix map.
mpls prefix-map	Configures a networking device to use a specified QoS map when a label destination prefix matches the specified access list.

mpls atm vpi

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm vpi** command is not available in Cisco IOS software.

To configure the range of values to use in the virtual path identifier (VPI) field for label virtual circuits (LVCs), use the **mpls atm vpi** command in interface configuration mode. To clear the range of values, use the **no** form of this command.

mpls atm vpi *vpi* [*- vpi*] [**vci-range** *low - high*]

no mpls atm vpi *vpi* [*- vpi*] [**vci-range** *low - high*]

Syntax Description

vpi	Virtual path identifier, low end of range (0 to 4095).
- vpi	(Optional) Virtual path identifier, high end of range (0 to 4095).
vci-range *low - high*	(Optional) Range of virtual channel identifier (VCI) values the subinterface can use for the VPI(s).

Defaults

The default VPI range is 1-1.

The default VCI range is 33-65535.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology. The **vci-range** keyword was added. The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

You might need to change the default VPI range on the switch if:

- It is an administrative policy to use a VPI value other than 1, the default VPI.
- There are many LVCs on an interface.

To configure ATM MPLS on a router interface (for example, an ATM Interface Processor), you must enable an MPLS subinterface.

Note The **mpls atm control-vc** and **mpls atm vpi** subinterface level configuration commands are available on any interface that can support ATM labeling.

Use this command to select an alternate range of VPI values for ATM label assignment on this interface. The two ends of the link negotiate a range defined by the intersection of the range configured at each end.

- To configure the VPI range for an edge label switch router (edge LSR) subinterface connected to another router or to an LSC, limit the range to four VPIs.
- For an ATM-LSR, the VPI range specified must lie within the range that was configured on the ATM switch for the corresponding ATM switch interface.
- If the LDP neighbor is a router, the VPI range can be no larger than two. For example, you can specify from 5 to 6 (a range of two), not 5 to 7 (a range of three). If the LDP neighbor is a switch, the maximum VPI range is 0 to 255.

If you use the **vci-range** keyword, you must specify a VPI value.

Examples

The following example shows how to create a subinterface and selects a VPI range from VPI 1 to VPI 3:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm vpi 1-3
```

The following example shows how to create a subinterface with a VPI of 240 and a VCI range between 33 and 4090:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm vpi 240 vci-range 33-4090
```

Related Commands

Command	Description
mpls atm control-vc	Configures VPI and VCI values for the initial link to an MPLS peer.

mpls atm vp-tunnel

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls atm vp-tunnel** command is not available in Cisco IOS software.

To specify an interface or a subinterface as a virtual path (VP) tunnel, use the **mpls atm vp-tunnel** command in interface configuration mode. To remove the VP tunnel from an interface or subinterface, use the **no** form of this command.

mpls atm vp-tunnel *vpi* [**vci-range** *low* - *high*]

no mpls atm vp-tunnel *vpi* [**vci-range** *low* - *high*]

Syntax Description

vpi	Virtual path identifier (VPI) value for the local end of the tunnel (0 to 4095).
vci-range *low* - *high*	(Optional) Range of virtual channel identifier (VCI) values the VP tunnel can use.

Defaults

If you do not specify a VCI range for the VP tunnel, the tunnel uses the default VCI range of 33-65535.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology. The **vci-range** keyword was added. The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

The **mpls atm vp-tunnel** and **mpls atm vpi** commands are mutually exclusive.

This command is available on both extended MPLS ATM (XTagATM) interfaces and on LC-ATM subinterfaces of router ATM interfaces. The command is not available on the LS1010, where all subinterfaces are automatically VP tunnels.

It is not necessary to use the **mpls atm vp-tunnel** command on an XTagATM interface in most applications. The switch learns (through VSI interface discovery) whether the XTagATM interface is a tunnel, the VPI value of the tunnel, and tunnel status.

Examples

The following example shows how to create an MPLS subinterface VP tunnel with a VPI value of 4:

```
Router(config-if)# mpls atm vp-tunnel 4
```

The following example shows how to create a VP tunnel with a value of 240 and a VCI range of 33 to 4090:

```
Router(config-if)# mpls atm vp-tunnel 240 vci-range 33-4090
```

mpls bgp forwarding

To enable an interface to receive Multiprotocol Label Switching (MPLS) packets when the signaling of MPLS labels is through the use of the Border Gateway Protocol (BGP), use the **mpls bgp forwarding** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

mpls bgp forwarding

no mpls bgp forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS forwarding by BGP is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

Use the **mpls bgp forwarding** command when you want to enable MPLS forwarding on directly connected loopback interfaces. This command is automatically generated by BGP for directly connected nonloopback neighbors.

Examples

The following example shows how to configure BGP to enable MPLS forwarding on a directly connected loopback interface, Ethernet 0/0:

```
interface ethernet 0/0
 mpls bgp forwarding
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

mpls control-word

To enable the Multiprotocol Label Switching (MPLS) control word in an Any Transport over MPLS (AToM) static pseudowire connection, use the **mpls control-word** command in xconnect configuration mode. To disable the control word, use the **no** form of this command.

mpls control-word

no mpls control-word

Syntax Description

This command has no arguments or keywords.

Command Default

The control word is included in connections.

Command Modes

Xconnect configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

This command is used when configuring AToM static pseudowires, and is mandatory when configuring Frame Relay data-link connection identifier (DLCI) and ATM adaptation layer 5 (AAL5) attachment circuits.

Because the control word is included by default, it may be necessary to explicitly disable this command in AToM static pseudowire configurations.

When the **mpls control-word** command is used in static pseudowire configurations, the command must be configured the same way on both ends of the connection to work correctly, or else the provider edge routers will not be able to exchange control messages to negotiate inclusion or exclusion of the control word.

Examples

The following example shows the configuration for both sides of an AToM static pseudowire connection:

```
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# no mpls control-word
Router(config-if-xconn)# exit
Router(config-if)# exit

Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
```

```
Router(config-if-xconn)# no mpls control-word
Router(config-if-xconn)# exit
Router(config-if)# exit
```

Related Commands

Command	Description
mpls label	Configures an AToM static pseudowire connection by defining local and remote pseudowire labels.
mpls label range	Configures the range of local labels available for use on packet interfaces.
show mpls l2transport vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.
xconnect	Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.

mpls cos-map

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls cos-map** command is not available in Cisco IOS software.

To create a class map that specifies how classes map to label virtual circuits (VCs) when they are combined with a prefix map, use the **mpls cos-map** command in global configuration mode.

mpls cos-map *cos-map*

Syntax Description

cos-map	Number from 1 to 155 that identifies the class map.

Defaults

No class maps are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.4(20)T	This command was removed.

Examples

The following example shows how to create a class map:

```
Router(config)# mpls cos-map 55
Router(config-mpls-cos-map)# class 1 premium
Router(config-mpls-cos-map)# exit
Router(config)#
```

Related Commands

Command	Description
mpls cos-map	Displays the QoS map used to assign a quantity of label virtual circuits and the associated class of service for those label virtual circuits.

mpls experimental

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **mpls experimental** command in VC-class configuration mode. To remove the MPLS EXP levels from the VC class, use the **no** form of this command.

To configure the MPLS EXP levels for a VC member of a bundle, use the **mpls experimental** command in bundle-vc configuration mode. To remove the MPLS EXP levels from the VC, use the **no** form of this command.

mpls experimental [**other** | *range*]

no mpls experimental

Syntax Description

other	(Optional) Specifies any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured. This is the default.
range	(Optional) A single MPLS EXP level specified as a number from 0 to 7, or a range of levels, specified as a hyphenated range.

Defaults

Defaults to **other**, that is, any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured.

Command Modes

VC-class configuration for a VC class (config-vc-class)
Bundle-vc configuration for ATM VC bundle members (config-if-atm-member)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(26)S	This command was implemented on the Cisco 10000 series router.
12.0(29)S	This command was integrated into Cisco IOS Release 12.0(29)S.
12.2(16)BC	This command was implemented on the ESR-PRE2.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines

Assignment of MPLS EXP levels to VC bundle members allows you to create differentiated service because you can distribute the MPLS EXP levels over the different VC bundle members. You can map a single level or a range of levels to each discrete VC in the bundle, thereby enabling VCs in the bundle to carry packets marked with different levels. Alternatively, you can configure a VC with the **mpls experimental other** command to indicate that it can carry traffic marked with levels not specifically configured for it. Only one VC in the bundle can be configured with the **mpls experimental other** command to carry all levels not specified. This VC is considered the default one.

To use this command in VC-class configuration mode, enter the **vc-class atm** global configuration command before you enter this command. This command has no effect if the VC class that contains the command is attached to a standalone VC, that is, if the VC is not a bundle member.

To use this command to configure an individual bundle member in bundle-VC configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-VC configuration mode.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest MPLS EXP level):

- VC configuration in bundle-VC mode
- Bundle configuration in bundle mode (with the effect of assigned VC class configuration)
- Subinterface configuration in subinterface mode

Note If you are using an ATM interface, you must configure all MPLS EXP levels (ranging from 0 to 7) for the bundle. For this configuration, Cisco recommends configuring one member of the bundle with the **mpls experimental other** command. The **other** keyword defaults to any MPLS EXP level in a range from 0 to 7 that is not explicitly configured.

Examples

The following example configures a class named control-class that includes an **mpls experimental** command that, when applied to a bundle, configures all VC members of that bundle to carry MPLS EXP level 7 traffic. Note that VC members of that bundle can be individually configured with the **mpls experimental** command at the bundle-vc level, which would supervene.

```
vc-class atm control-class
 mpls experimental 7
```

The following example configures a permanent virtual circuit (PVC) 401, named control-class, to carry traffic with MPLS EXP levels in the range of 4 to 2, overriding the level mapping set for the VC through VC-class configuration:

```
pvc-bundle control-class 401
 mpls experimental 4-2
```

Related Commands

Command	Description
bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
bundle	Creates a bundle or modifies an existing bundle, and enters bundle configuration mode.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
pvc-bundle	Adds a VC to a bundle as a member and enters bundle-VC configuration mode to configure that VC bundle member.
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-nrt QoS and specifies the output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
vc-class atm	Creates a VC class for an ATM PVC, SVC, or ATM interface, and enters VC-class configuration mode.

mpls export interval

To configure the collection and export of Multiprotocol Label Switching (MPLS) Prefix/Application/Label (PAL) information to a NetFlow collector, use the **mpls export interval** command in global configuration mode. To disable the collecting and exporting of the MPLS PAL information, use the **no** form of this command.

mpls export interval *interval*

no mpls export interval

Syntax Description

interval	Specifies the time interval in minutes between full MPLS PAL table exports. The range of valid time intervals is 0 to 10080 minutes.

Command Default

No capture or export of PAL table entries is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure the collection and export of MPLS PAL information to a NetFlow collector. The collector can be the Cisco NetFlow Collection Engine or a third-party collector application.

The *interval* argument specifies the number of minutes between one export of the entire MPLS PAL table and the next export of the entire table. We recommend that you select a time interval from 360 minutes (6 hours) to 1440 minutes (24 hours) depending on the size of your network. If you want to trigger an immediate export of the PAL table, disable the functionality (**no mpls export interval** command) and reconfigure the command with an interval argument greater than zero.

If you enter the command with a periodic interval of zero, entries of the MPLS PAL table are not exported repeatedly, but PAL label tracking still occurs and PAL information is exported to the collector when a label is allocated. To display the entire MPLS PAL table, use the **show mpls flow mappings** command.

The *interval* argument that you specify is the least amount of time that passes before another export of the MPLS PAL table. The system might choose to delay the MPLS PAL table export, if the PAL export queue already contains a large number of entries. This might occur if the export queue contains tens of thousands of entries, for example, if the export occurred at a time when thousands of routes just came up, or if NetFlow did not have the time to clear the export queue from either a previous export of the full table or a previous time when thousands of routes came up in a brief period.

Examples

The following example shows how to configure a time interval of 720 minutes (12 hours) between exports of the entire MPLS PAL table to a NetFlow collector:

```
configure terminal
 mpls export interval 720
 exit
```

Related Commands

Command	Description
mpls export vpnv4 prefixes	Configures the tracking and export of VPNv4 label information from the MPLS PAL table to a NetFlow collector.
show mpls flow mappings	Displays all entries in the MPLS PAL table.

mpls export vpnv4 prefixes

To configure the tracking and export of Virtual Private Network (VPN) IPv4 (VPNv4) label information from the Multiprotocol Label Switching (MPLS) Prefix/Application/Label (PAL) table to a NetFlow collector, use the **mpls export vpnv4 prefixes** command in global configuration mode. To disable the tracking and exporting of VPNv4 label information, use the **no** form of this command.

mpls export vpnv4 prefixes

no mpls export vpnv4 prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

VPNv4 labels are exported from the MPLS PAL table with a destination prefix of 0.0.0.0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable the tracking and export of VPNv4 label information from the MPLS PAL table.

In MPLS PAL table records, the default prefix stored for labels allocated by VPNs, Border Gateway Protocol (BGP) IPv4, or BGP VPNv4 is intentionally 0.0.0.0. This is because VPN prefixes might be reused; Other VPNs might use the same prefix.

If you configure the **mpls export vpnv4 prefixes** command, the MPLS PAL table stores the VPN prefix and its associated route distinguisher (RD). The use of an RD removes any ambiguity among VPN prefixes. Even if IP addresses are reused, the addition of an RD creates a prefix unique.

Examples

The following example shows how to configure the tracking and exporting of VPNv4 label information from the MPLS PAL table to a NetFlow collector:

```
configure terminal
 mpls export interval 720
 mpls export vpnv4 prefixes
 exit
```

The full MPLS PAL table with MPLS VPNv4 label information is configured to export to the NetFlow collector every 720 minutes (12 hours).

Related Commands

Command	Description
mpls export interval	Configures the collection and export of MPLS PAL information to a NetFlow collector.
show mpls flow mappings	Displays all entries in the MPLS PAL table.

mpls forwarding bgp

To enable Multiprotocol Label Switching (MPLS) nonstop forwarding on an interface that uses Border Gateway Protocol (BGP) as the label distribution protocol, use the **mpls forwarding bgp** command in interface configuration mode. To disable MPLS nonstop forwarding on the interface, use the **no** form of this command.

mpls forwarding bgp

no mpls forwarding bgp

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS nonstop forwarding is not enabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Configure this command on the interfaces of the BGP peers that send and receive labels. If this command is not configured on an interface and a stateful switchover occurs, packets received from an interface are dropped until the BGP session is established in the new route processor.

Issue this command to enable nonstop forwarding on interfaces that use BGP to distribute labels for the following types of VPNs:

- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

Examples

In the following examples, an interface is configured to save BGP labels in the event of a stateful switchover:

Cisco 7000 Series Example

```
Router(config)# interface Pos1/0
Router(config-if)# mpls forwarding bgp
```

Cisco 10000 Series Example

```
Router(config)# interface Pos1/0/0
Router(config-if)# mpls forwarding bgp
```

Related Commands

Command	Description
bgp graceful-restart	Enables BGP Graceful Restart on the router.

mpls ip (global configuration)

To enable Muliprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths for the platform, use the **mpls ip** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ip

no mpls ip

Syntax Description

This command has no arguments or keywords.

Defaults

Label switching of IPv4 packets along normally routed paths is enabled for the platform.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths (sometimes called dynamic label switching) is enabled by this command. For a given interface to perform dynamic label switching, this switching function must be enabled for the interface and for the platform.

The **no** form of this command stops dynamic label switching for all platform interfaces regardless of the interface configuration; it also stops distribution of labels for dynamic label switching. However, the **no** form of this command does not affect the sending of labeled packets through label switch path (LSP) tunnels.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) originating at, terminating at, or passing through the platform.

Examples

The following example shows that dynamic label switching is disabled for the platform, and all label distribution is terminated for the platform:

```
Router(config)# no mpls ip
```

Related Commands

Command	Description
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the associated interface.

mpls ip (interface configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths for a particular interface, use the **mpls ip** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

mpls ip

no mpls ip

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS forwarding of IPv4 packets along normally routed paths for the interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching has been enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the **no** form of the command does not affect the sending of labeled packets through any link-state packet (LSP) tunnels that might use the interface.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) beginning at, terminating at, or passing through the interface.

Examples

The following example shows how to enable label switching on the specified Ethernet interface:

```
Router(config)# configure terminal
Router(config-if)# interface e0/2
Router(config-if)# mpls ip
```

Related Commands

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the downstream on demand method of label distribution.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.

mpls ip default-route

To enable the distribution of labels associated with the IP default route, use the **mpls ip default-route** command in global configuration mode.

mpls ip default-route

Syntax Description

This command has no arguments or keywords.

Defaults

No distribution of labels for the IP default route.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was modified to reflect new Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Dynamic label switching (that is, distribution of labels based on routing protocols) must be enabled before you can use the **mpls ip default-route** command.

Examples

The following example shows how to enable the distribution of labels associated with the IP default route:

```
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls ip default-route
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.

mpls ip encapsulate explicit-null

To encapsulate all packets forwarded from the interface or subinterface with an explicit NULL label header, use the **mpls ip encapsulate explicit-null** command in interface configuration or subinterface configuration mode. To disable this function, use the **no** form of this command.

mpls ip encapsulate explicit-null

no mpls ip encapsulate explicit-null

Syntax Description

This command has no arguments or keywords.

Defaults

Packets are sent out without an explicit NULL label header.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This is a per-interface command. The command establishes an explicit NULL LSP at the customer edge (CE) router. If MPLS is configured on a router and you enter this command, an error message occurs. This command is also supported on the Cisco 2600 series and Cisco 3600 series platforms.

Examples

The following example shows how to encapsulate all packets forwarded onto the interface or subinterface with an explicit NULL label header:

```
Router(config-if)# mpls ip encapsulate explicit-null
```

mpls ip propagate-ttl

To control the generation of the time-to-live (TTL) field in the Multiprotocol Label Switching (MPLS) header when labels are first added to an IP packet, use the **mpls ip propagate-ttl** command in global configuration mode. To use a fixed TTL value (255) for the first label of the IP packet, use the **no** form of this command.

mpls ip propagate-ttl

no mpls ip propagate-ttl [**forwarded** | **local**]

Syntax Description

forwarded	(Optional) Prevents the **traceroute** command from showing the hops for forwarded packets.
local	(Optional) Prevents the **traceroute** command from showing the hops only for local packets.

Defaults

This command is enabled. The TTL field is copied from the IP header. A **traceroute** command shows all of the hops in the network.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.1(5)T	The keywords **forwarded** and **local** were added to this command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, the **mpls ip propagate-ttl** command is enabled and the IP TTL value is copied to the MPLS TTL field during label imposition. To disable TTL propagation for all packets, use the **no mpls ip propagate-ttl** command. To disable TTL propagation for only forwarded packets, use the **no mpls ip propagate forwarded** command. Disabling TTL propagation of forwarded packets allows the structure of the MPLS network to be hidden from customers, but not the provider.

This feature supports the IETF draft document *ICMP Extensions for Multiprotocol Label Switching*, draft-ietf-mpls-label-icmp-01.txt. The document can be accessed at the following URL:

http://www2.ietf.org/internet-drafts/draft-ietf-mpls-label-icmp-01.txt

Examples

The following example shows how to disable the TTL field in the MPLS header for only forwarded packets:

```
Router(config)# no mpls ip propagate-ttl forwarded
```

Related Commands

Command	Description
traceroute	Displays the routes that packets take through a network to their destinations.

mpls ip ttl-expiration pop

To specify how a packet with an expired time-to-live (TTL) value is forwarded, use the **mpls ip ttl-expiration pop** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls ip ttl-expiration pop *labels*

no mpls ip ttl-expiration pop *labels*

Syntax Description

labels	The maximum number of labels in the packet necessary for the packet to be forwarded by means of the global IP routing table.

Defaults

The packets are forwarded by the original label stack. However, in previous versions of Cisco IOS software, the packets were forwarded by the global routing table by default.

12.0S	Packets are forwarded through the use of the global routing table.
12.0ST	Packets are forwarded through the use of the original label stack.
12.1T	Packets are forwarded through the use of the original label stack.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify that the packet be forwarded by the global IP routing table or by the packet's original label stack. The forwarding method is determined by the number of labels in the packet. You specify the number of labels as part of the command. If the packet contains the same or fewer labels than you specified, it is forwarded through the use of the global IP routing table. If the packet contains more labels than you specified, the packet is forwarded through the use of the original label stack.

This command is useful if expired TTL packets do not get back to their source, because there is a break in the Interior Gateway Protocol (IGP) path. Currently, MPLS forwards the expired TTL packets by reimposing the original label stack and forwarding the packet to the end of a label switched path (LSP). (For provider edge routers forwarding traffic over a Virtual Private Network (VPN), this is the only way to get the packet back to the source.) If there is a break in the IGP path to the end of the LSP, the packet never reaches its source.

If packets have a single label, that label is usually a global address or terminal VPN label. Those packets can be forwarded through the use of the global IP routing table. Packets that have more than one label can be forwarded through the use of the original label stack. Enter the **mpls ip ttl-expiration pop 1** command to enable forwarding based on more than one label. (This is the most common application of the command.)

Examples

The following example shows how to enable forwarding based on more than one label:

```
Router(config)# mpls ip ttl-expiration pop 1
```

Related Commands

Command	Description
traceroute	Displays the routes that packets take through a network to their destinations.

mpls ipv6 source-interface

Note Effective with Cisco IOS Release 12.2(25)S, the **mpls ipv6 source-interface** command is not available in Cisco IOS 12.2S releases.
Effective with Cisco IOS Release 12.4(15)T, the **mpls ipv6 source-interface** command is not available in Cisco IOS 12.4T releases.

To specify an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over a Multiprotocol Label Switching (MPLS) network, use the **mpls ipv6 source-interface** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ipv6 source-interface *type number*

no mpls ipv6 source-interface

Syntax Description

type number	The interface type and number whose IPv6 address is to be used as the source for locally generated IPv6 packets to be sent over an MPLS backbone. **Note** A space between the *type* and *number* arguments is not required.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(20)S	This command was integrated into Cisco IOS Release 12.2(20)S.
12.2(25)S	This command was removed from Cisco IOS Release 12.2(25)S.
12.4(15)T	This command was removed from Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **mpls ipv6 source-interface** command with the **neighbor send-label** address family configuration command to allow IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers, configured to run both IPv4 and IPv6, forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

The **mpls ipv6 source-interface** command was removed from Cisco IOS software as per RFC 3484, which defines how the source address of a locally generated packet must be chosen. This command will be removed from the other Cisco IOS release trains in which it currently appears.

Examples

The following example shows loopback interface 0 being configured as a source address for locally generated IPv6 packets:

```
interface Loopback0
 ip address 192.168.99.5 255.255.255.255
 ipv6 address 2001:0DB8::1/32
!
mpls ipv6 source-interface loopback0
```

Related Commands

Command	Description
neighbor send-label	Advertises the capability of the router to send MPLS labels with BGP routes.

mpls l2transport route

To enable routing of Any Transport over MPLS (AToM) packets over a specified virtual circuit (VC), use the **mpls l2transport route** command in the appropriate command mode. To delete the VC, use the **no** form of this command on both provider edge (PE) routers.

mpls l2transport route *destination vc-id*

no mpls l2transport route *destination vc-id*

Syntax Description

destination	Specifies the Label Distribution Protocol (LDP) IP address of the remote PE router.
vc-id	Assigns a VC number to the virtual circuit between two PE routers.

Defaults

Routing of MPLS packets over a specified VC is disabled.

Command Modes

Depending on the AToM transport type you are configuring, you use the **mpls l2transport route** command in one of the following command modes:

Transport Type	Command Mode
ATM AAL5 and cell relay	ATM VC configuration mode
Ethernet VLAN	Subinterface or interface configuration mode
Frame Relay	Connect submode
HDLC and PPP	Interface configuration mode

Command History

Release	Modification
12.1(8a)E	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A Multiprotocol Label Switching (MPLS) VC runs across an MPLS cloud to connect interfaces on two PE routers.

Use this command on each PE router to route packets across the MPLS cloud to the interface of the other PE router. Specify the LDP IP address of the other PE router for the *destination* parameter. Do not specify the IP address of the router from which you are issuing the command.

You can choose any number for the VC ID. However, the VC ID must be unique per pair of routers. Therefore, in large networks, it may be necessary to track the VC ID assignments to ensure that a VC ID does not get assigned twice.

Cisco 7600 Series Routers

Cisco 7600 series routers equipped with a Supervisor Engine 2 must be equipped with either an optical services module (OSM) or a FlexWAN port adapter that is facing the MPLS network with a Layer 2 Ethernet port (non-OSM) facing the customer.

The **mpls l2transport route** command enables the virtual connection used to route the VLAN packets. The types of virtual connections used are as follows:

- VC Type 4—Allows all the traffic in a VLAN to use a single VC across the MPLS network.
- VC Type 5—Allows all traffic on a port to share a single VC across the MPLS network.

During the VC setup, VC type 5 is advertised. If the peer advertises VC type 4, the VC type is changed to type 4 and the VC is restarted. The change only happens from type 5 to type 4 and never from type 4 to type 5.

An MPLS VLAN virtual circuit in Layer 2 runs across an MPLS cloud to connect the VLAN interfaces on two PE routers.

Use the **mpls l2transport route** command on the VLAN interface of each PE router to route the VLAN packets in Layer 2 across the MPLS cloud to the VLAN interface of the other PE router. Specify the IP address of the other PE router for the destination parameter. Do not specify the IP address of the router from which you are issuing the command.

You can choose any value for the virtual-connection ID. However, the virtual-circuit ID must be unique to each virtual connection. In large networks, you may need to track the virtual-connection ID assignments to ensure that a virtual-connection ID does not get assigned twice.

The routed virtual connections are supported on the main interfaces, not subinterfaces.

Examples

The following examples show how to enable routing of MPLS packets over a specified VC. Two routers named PE1 and PE2 establish a VC to transport packets. PE1 has IP address 172.16.0.1, and PE2 has IP address 192.168.0.1. The VC ID is 50.

ATM AAL5 over MPLS Example

At PE1, you issue the following commands:

```
PE1_Router(config)# interface atm5/0.100
PE1_Router(config-if)# pvc 1/200
PE1_Router(config-atm-vc)# encapsulation aal5
PE1_Router(config-atm-vc)# mpls l2transport route 192.168.0.1 50
```

At PE2, you issue the following commands:

```
PE2_Router(config)# interface atm5/0.100
PE2_Router(config-if)# pvc 1/200
PE2_Router(config-atm-vc)# encapsulation aal5
PE2_Router(config-atm-vc)# mpls l2transport route 172.16.0.1 50
```

ATM Cell Relay over MPLS Example

At PE1, you issue the following commands:

```
PE1_Router(config)# interface atm5/0.100
PE1_Router(config-if)# pvc 1/200 l2transport
PE1_Router(config-atm-vc)# encapsulation aal0
PE1_Router(config-atm-vc)# mpls l2transport route 192.168.0.1 50
```

At PE2, you issue the following commands:

```
PE2_Router(config)# interface atm5/0.100
PE2_Router(config-if)# pvc 1/200 l2transport
PE2_Router(config-atm-vc)# encapsulation aal0
PE2_Router(config-atm-vc)# mpls l2transport route 172.16.0.1 50
```

Ethernet over MPLS Example

At PE1, you issue the following commands:

```
PE1_Router(config)# interface GigabitEthernet1/0.2
PE1_Router(config-subif)# encapsulation dot1Q 200
PE1_Router(config-subif)# mpls l2transport route 192.168.0.1 50
```

At PE2, you issue the following commands:

```
PE2_Router(config)# interface GigabitEthernet2/0.1
PE2_Router(config-subif)# encapsulation dot1Q 200
PE2_Router(config-subif)# mpls l2transport route 172.16.0.1 50
```

Frame Relay over MPLS Example

At PE1, you issue the following commands:

```
PE1_Router(config)# connect frompls1 Serial5/0 1000 l2transport
PE1_Router(config-fr-pw-switching)# mpls l2transport route 192.168.0.1 50
```

At PE2, you issue the following commands:

```
PE2_Router(config)# connect frompls2 Serial2/0 102 l2transport
PE2_Router(config-fr-pw-switching)# mpls l2transport route 172.16.0.1 50
```

HDLC over MPLS Example

At PE1, you issue the following commands:

```
PE1_Router(config)# interface Serial3/0
PE1_Router(config-if)# encapsulation hdlc
PE1_Router(config-if)# mpls l2transport route 192.168.0.1 50
```

At PE2, you issue the following commands:

```
PE2_Router(config)# interface Serial1/0
PE2_Router(config-if)# encapsulation hdlc
PE2_Router(config-if)# mpls l2transport route 172.16.0.1 50
```

PPP over MPLS Example

At PE1, you issue the following commands:

```
PE1_Router(config)# interface Serial3/0
PE1_Router(config-if)# encapsulation ppp
PE1_Router(config-if)# mpls l2transport route 192.168.0.1 50
```

At PE2, you issue the following commands:

```
PE2_Router(config)# interface Serial1/0
PE2_Router(config-if)# encapsulation ppp
PE2_Router(config-if)# mpls l2transport route 172.16.0.1 50
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

mpls label

To configure an Any Transport over MPLS (AToM) static pseudowire connection by defining local and remote circuit labels, use the **mpls label** command in xconnect configuration mode. To remove the local and remote pseudowire labels, use the **no** form of this command.

mpls label *local-pseudowire-label remote-pseudowire-label*

no mpls label

Syntax Description

local-pseudowire-label	An unused static label that is within the range defined by the **mpls label range** command.
remote-pseudowire-label	The value of the peer provider edge router's local pseudowire label.

Command Default

No default labels.

Command Modes

Xconnect configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

This command is mandatory when configuring AToM static pseudowires, and must be configured at both ends of the connection.

The **mpls label** command checks the validity of the local pseudowire label and will generate an error message if the label is invalid.

Examples

The following example shows configurations for both ends of an AToM static pseudowire connection:

```
Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# exit
Router(config-if)# exit

Router# configure terminal
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
Router(config-if-xconn)# exit
Router(config-if)# exit
```

Related Commands

Command	Description
mpls control-word	Enables sending the MPLS control word in an AToM static pseudowire connection.
mpls label range	Configures the range of local labels available for use on packet interfaces.
show mpls l2transport vc	Displays information about AToM VCs and AToM static pseudowires that have been enabled to route Layer 2 packets on a router.
xconnect	Binds an attachment circuit to a pseudowire, and configures an AToM static pseudowire.

mpls label mode

To configure the Per VRF Labels, use the **mpls label mode** command in global configuration mode. To disable the Per VRF Label feature, use the **no** form of this command.

mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol bgp-vpnv4** {**per-prefix** | **per-vrf**}

no mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol bgp-vpnv4** {**per-prefix** | **per-vrf**}

Syntax Description

vrf	Configures a single VPN routing and forwarding (VRF) domain.
vrf-name	Specifies a name for the single VRF you want to configure.
all-vrfs	Configures a label mode for all VRFs on the router.
protocol	Specifies a protocol to use for the label mode.
bgp-vpnv4	Specifies the IPv4 VRF Address-family protocol for the label mode configuration.
per-prefix	Specifies per-prefix label mode.
per-vrf	Specifies per-vrf label mode.

Command Default

Per-vrf-aggr label mode is the default for connected routes and Border Gateway Protocol (BGP) aggregate routes on the Cisco 6500 router. Per-prefix label mode is the default for all other local routes.

Command Modes

Global configuration (config)#

Command History

Release	Modification
XE Release 2.2	This command was introduced.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Examples

The following command example configures all VRFs to per-vrf mode:

```
Router(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
```

Related Commands

Command	Description
debug ip bgp vpnv4 unicast	Displays debugging messages for VPNv4 unicast routes.
show ip vrf detail	Displays the assigned label mode for the VRF.

mpls label mode (6VPE)

To configure the MPLS VPN 6VPE per VRF Label feature, use the **mpls label mode** command in global configuration mode. To disable the MPLS VPN 6VPE per VRF Label feature, use the **no** form of this command.

mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol** {**bgp-vpnv6** | **all-afs**} {**per-prefix** | **per-vrf**}

no mpls label mode {**vrf** *vrf-name* | **all-vrfs**} **protocol** {**bgp-vpnv6** | **all-afs**} {**per-prefix** | **per-vrf**}

Syntax Description

vrf *vrf-name*	Configures a single VPN routing and forwarding (VRF) domain. • *vrf-name*—The name for the single VRF you want to configure.
all-vrfs	Configures a label mode for all VRFs on the router.
protocol	Specifies a protocol to use for the label mode. • **bgp-vpnv6**—Specifies the IPv6 VRF address-family protocol for the label mode configuration. • **all-afs**—Configures a label mode for all address families (AFs) on the router. – If a VRF is configured with the **all-afs** label mode, you cannot change the label mode for individual AFs. To configure each of the AFs for different label modes, you must first remove the **all-afs** mode keyword. Similarly, if individual AFs are configured with different label modes, the **all-afs** label mode for the VRF is not accepted. – The **all-afs** label mode keyword has higher precedence over the individual AF label mode keywords (**vrf** or **all-vrfs**).
per-prefix	Specifies per-prefix label mode.
per-vrf	Specifies per-vrf label mode.

Command Default

The command default for connected routes and Border Gateway Protocol (BGP) aggregate routes on the Cisco 7600 router is **Per-vrf-aggr** label mode. The command default for all other local routes is **Per-prefix** label mode.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(33)SRD	This command was introduced.

Examples

The following example configures all VRFs to per-vrf mode:

```
Router(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
```

Related Commands

Command	Description
debug ip bgp vpnv6 unicast	Displays debugging messages for VPNv6 unicast routes.
show vrf detail	Displays the assigned label mode for the VRF.

mpls label protocol (global configuration)

To specify the Label Distribution Protocol (LDP) for a platform, use the **mpls label protocol** command in global configuration mode. To restore the default LDP, use the **no** form of this command.

mpls label protocol {**ldp** | **tdp**}

no mpls label protocol

Syntax Description

ldp	Specifies that LDP is the default label distribution protocol.
tdp	Specifies that Tag Distribution Protocol (TDP) is the default label distribution protocol.

Command Default

LDP is the default label distribution protocol.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4(3)	The command default changed from TDP to LDP.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If neither the global **mpls label protocol ldp** command nor the interface **mpls label protocol ldp** command is used, all label distribution sessions use LDP.

Note 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.

Examples

The following command establishes LDP as the label distribution protocol for the platform:

```
Router(config)# mpls label protocol ldp
```

Related Commands

Command	Description
mpls idp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.
show mpls interfaces	Displays information about one or more or all interfaces that are configured for label switching.

mpls label protocol (interface configuration)

To specify the label distribution protocol for an interface, use the **mpls label protocol** command in interface configuration mode. To remove the label distribution protocol from the interface, use the **no** form of this command.

mpls label protocol {**ldp** | **tdp** | **both**}

no mpls label protocol

Syntax Description

ldp	Specifies that the label distribution protocol (LDP) is to be used on the interface.
tdp	Specifies that the tag distribution protocol (TDP) is to be used on the interface.
both	Specifies that both label and tag distribution protocols are to be supported on the interface.

Command Default

If no protocol is explicitly configured for an interface, the label distribution protocol that was configured for the platform is used. To set the platform label distribution protocol, use the global **mpls label protocol** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

To successfully establish a session for label distribution for a link connecting two label switch routers (LSRs), the link interfaces on the LSRs must be configured to use the same label distribution protocol. If there are multiple links connecting two LSRs, all of the link interfaces connecting the two LSRs must be configured to use the same protocol.

The **both** option is intended for use with interfaces to multiaccess networks, such as Ethernet and FDDI, where some peers might use LDP and others use TDP. When you specify the **both** option, the LSR sends both LDP and TDP discovery hello messages and responds to both types of messages.

Examples

The following example shows how to establish LDP as the label distribution protocol for the interface:

```
Router(config-if)# mpls label protocol ldp
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more interfaces that are configured for label switching.

mpls label range

To configure the range of local labels available for use with Multiprotocol Label Switching (MPLS) applications on packet interfaces, use the **mpls label range** command in global configuration mode. To revert to the platform defaults, use the **no** form of this command.

mpls label range *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*]

no mpls label range

Syntax Description

minimum-value	The value of the smallest label allowed in the label space. The default is 16.
maximum-value	The value of the largest label allowed in the label space. The default is platform-dependent.
static	(Optional) Reserves a block of local labels for static label assignments. If you omit the **static** keyword and the *minimum-static-value* and *maximum-static-value* arguments, no labels are reserved for static assignment.
minimum-static-value	(Optional) The minimum value for static label assignments. There is no default value.
maximum-static-value	(Optional) The maximum value for static label assignments. There is no default value.

Command Default

The platform's default values are used.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was modified to use the new MPLS Internet Engineering Task Force (IETF) terminology and command-line interface (CLI) syntax.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. The **static** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(16)	The output was modified to display the upper and lower minimum static label values in the help lines instead of the default range.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The default values for the following arguments were modified: *maximum-value*, *minimum-static-value*, and *maximum-static-value*. The "Usage Guidelines" changed.

Usage Guidelines

The labels 0 through 15 are reserved by the IETF (see RFC 3032, MPLS Label Stack Encoding, for details) and cannot be included in the range specified in the **mpls label range** command. If you enter a 0 in the command, you will get a message that indicates that the command is an unrecognized command.

The label range defined by the **mpls label range** command is used by all MPLS applications that allocate local labels (for dynamic label switching, MPLS traffic engineering, MPLS Virtual Private Networks (VPNs), and so on).

If you specify a new label range that does not overlap the range currently in use, the new range does not take effect until you reload the router or the router undergoes a Stateful Switchover (SSO) when you are using Cisco IOS Release 12.0S and older software. Later software with the new MPLS Forwarding Infrastructure (MFI), 12.2SR, 12.2SB, 12.2(33)XHI, 12.2(25)SE, and 12.5 allows immediate use of the new range. Existing label bindings, which may violate the newly-configured ranges, remain active until the binding is removed through other methods.

You can use label distribution protocols, such as Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP), to reserve a generic range of labels from 16 through 1048575 for dynamic assignment.

You specify the optional keyword, **static**, to reserve labels for static assignment. The MPLS Static Labels feature requires that you configure a range of labels for static assignment. You can configure static bindings only from the current static range. If the static range is not configured or is exhausted, then you cannot configure static bindings.

The available range of label values is from 16 to 1048575. The maximum value defaults to 1048575, but might be limited to a lower value on certain platforms. Some platforms may support only 256,000 or 512,000 labels. Refer to your platform documentation for the default maximum label value.

If you configure the dynamic label space from 16 to 1048575, the static label space can be in a range that is outside the chosen dynamic label space. The upper and lower minimum static label values are displayed in the help line. For example, if you configure the dynamic label with a minimum value of 100 and a maximum value of 1000, the help lines display as follows:

```
Router(config)# mpls label range 100 1000 static ?

<1001-1048575>  Upper Minimum static label value
<16-99>         Lower Minimum static label value

Reserved Label Range  --> 0    to 15
Available Label Range --> 16   to 1048575
Dynamic Label Range   --> 100  to 1000
Lower End Range       --> 16   to 99
Upper End Range       --> 1001 to 1048575
```

In this example, you can configure a static range from one of the following ranges: 16 to 99 or 1001 to 1048575.

If the lower minimum static label space is not available, the lower minimum is not displayed in the help line. For example:

```
Router(config)# mpls label range 16 400 static ?

  <401-1048575>  Upper Minimum static label value
```

In this example, you can configure a static range with a minimum static value of 401 and a maximum static value of up to 1048575.

If an upper minimum static label space is not available, then the upper minimum is not displayed in the help line:

```
Router(config)# mpls label range 1000 1048575 static ?
```

```
  <16-999>  Lower Minimum static label value
```

In this example, the range available for static label assignment is from 16 to 999.

If you configure the dynamic label space with the default minimum (16) and maximum (1048575) values, no space remains for static label assignment, help lines are not displayed, and you cannot configure static label bindings. For example:

```
Router(config)# mpls label range 16 1048575 ?

  <cr>
```

Examples

The following example shows how to configure the size of the local label space. In this example, the minimum static value is set to 200, and the maximum static value is set to 120000.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# mpls label range 200 120000
Router(config)#
```

If you had specified a new range that overlaps the current range (for example, the new range of the minimum static value set to 16 and the maximum static value set to 120000), then the new range takes effect immediately.

The following example show how to configure a dynamic local label space with a minimum static value set to 1000 and the maximum static value set to 1048575 and a static label space with a minimum static value set to 16 and a maximum static value set to 999:

```
Router(config)# mpls label range 1000 1048575 static 16 999
Router(config)#
```

In the following output, the **show mpls label range** command, executed after a reload, shows that the configured range is now in effect:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 1000/1048575
Range for static labels: Min/Max/Number: 16/999
```

The following example shows how to restore the label range to its default value:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# no mpls label range
Router(config)# end
```

Related Commands

Command	Description
show mpls forwarding table	Displays the contents of the MPLS LFIB.
show mpls label range	Displays the range of the MPLS local label space.

mpls ldp address-message

To specify advertisement of platform addresses to an LC-ATM label distribution protocol (LDP) peer, use the **mpls ldp address-message** command in interface configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp address-message

no mpls ldp address-message

Syntax Description

This command has no arguments or keywords.

Defaults

LDP Address and Address Withdraw messages are not sent to LC-ATM LDP peers.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The LDP specification includes Address and Address Withdraw messages used by a label switch router (LSR) to advertise its addresses to its peers.

An LSR uses the addresses it learns from peers when operating in Downstream Unsolicited label advertisement mode to convert between route next hop addresses (found in the LSR routing table) and peer LDP identifiers.

The ability to map between the IP address and the peer LDP identifier is required so that:

- When the Multiprotocol Label Swithcing (MPLS) forwarding engine (the Label Forwarding Information Base [LFIB]) asks for labels for a given destination prefix and next hop address, the LSR can find the label learned (if any) from the next hop. The LSR maintains learned labels in its label information base (LIB) tagged by the LDP ID of the advertising LSR.
- When the LSR learns a label for destination prefix P from an LDP peer, it can determine if that peer (known to the LSR by its LDP identifier) is currently the next hop for P.

In principle, an LSR operating in Downstream On Demand (DoD) mode for an LC-ATM interface does not need this information for two reasons:

- The LSR should know from the routing table the next hop interface.
- Only one DoD peer exists per LC-ATM interface.

Consequently, Cisco platforms do not normally send Address and Address Withdraw messages to LC-ATM peers.

Some LDP implementations might require the information learned in Address and Address Withdraw messages for LC-ATM. The **mpls ldp address-message** command is provided to enable interoperability with implementation vendors that require Address messages for LC-ATM.

Note Cisco platforms always advertise their addresses in Address and Address Withdraw messages for LDP sessions operating in Downstream Unsolicited label advertisement mode.

Examples

The following is an example of the **mpls ldp address-message** command:

```
Router(config-if)# mpls ldp address-message
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more or all interfaces that are configured for label switching.

mpls ldp advertise-labels

To control the distribution of locally assigned (incoming) labels by means of label distribution protocol (LDP), use the **mpls ldp advertise-labels** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp advertise-labels [**vrf** *vpn-name*] [**interface** *interface* | **for** *prefix-access-list* [**to** *peer-access-list*]]

no mpls ldp advertise-labels [**vrf** *vpn-name*] [**interface** *interface* | **for** *prefix-access-list* [**to** *peer-access-list*]]

Syntax Description

vrf *vpn-name*	(Optional) Specifies the Virtual Private Network (VPN) routing and forwarding (VFR) instance for label advertisement.
interface *interface*	(Optional) Specifies an interface for label advertisement of an interface address.
for *prefix-access-list*	(Optional) Specifies which destinations should have their labels advertised.
to *peer-access-list*	(Optional) Specifies which LDP neighbors should receive label advertisements. An LSR is identified by its router ID, which consists of the first 4 bytes of its 6-byte LDP identifier.

Defaults

The labels of all destinations are advertised to all LDP neighbors.
If the **vrf** keyword is not specified, this command applies to the default routing domain.
If the **interface** keyword is not specified, no label is advertised for the interface address.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect Mutiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP and to make the command consistent with the way Cisco IOS software interprets the *prefix-access-list* argument.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.(22)S. The **interface** *interface* keyword and argument were added.

Release	Modification
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to control which labels are advertised to which LDP neighbors. To prevent the distribution of any locally assigned labels, use the **no mpls ldp advertise-labels** command with no optional parameters. To reenable the distribution of all locally assigned labels to all LDP neighbors, use the **mpls ldp advertise-labels** command with no optional parameters.

You can execute multiple **mpls ldp advertise-labels** commands. In the aggregate, such commands determine how the LSR advertises local labels. The following rules describe the effects of multiple commands:

1. Every **mpls ldp advertise-labels** command has a *(prefix acl, peer acl)* pair associated with it. The *access list* pair associated with the **mpls ldp advertise-labels** command (in the absence of both the **for** and **to** keywords) is *(none, none)*; the *access list* pair associated with the **mpls ldp advertise-labels for** *prefix acl* command (in the absence of the **to** keyword) is *(prefix-acl, none)*.
2. A given prefix can have, at most, one *(prefix acl, peer acl)* pair that "applies" to it, as in the following explaination:
   a. A given (*prefix acl, peer acl*) pair "applies" to a prefix only if the *prefix acl* "matches" the prefix. A match occurs if the *prefix acl* permits the prefix.
   b. If more than one *(prefix acl, peer acl)* pair from multiple **mpls ldp advertise-labels** commands matches a prefix, the *(prefix acl, peer acl)* pair in the first such command (as determined by the **show running** command**)** "applies" to the prefix.
3. When an LSR is ready to advertise a label for a prefix, the LSR:
   a. Determines whether a *(prefix acl, peer acl)* pair applies to the prefix.
   b. If none applies, and if the **no mpls ldp advertise-labels** command has been configured, the label for the prefix is not advertised to any peer; otherwise, the label is advertised to all peers.
   c. If a *(prefix acl, peer acl)* pair applies to the prefix, and if the *prefix acl* "denies" the prefix, the label is not advertised to any peer.
   d. If the *prefix acl* "permits" the prefix and the *peer acl* is *none* (that is, the command that "applies" to the prefix is an **mpls ldp advertise-labels for** *prefix acl* command without the **to** keyword), then the label is advertised to all peers.
   e. If the *prefix acl* "permits" the prefix and there is a *peer acl*, then the label is advertised to all peers permitted by the *peer acl*.

Note The **mpls ldp advertise-labels** command has no effect on an LC-ATM interface. Such an interface behaves as though this command had not been executed.

Normally, LDP advertises labels only for IP prefixes that are in the routing table. You can use the **mpls ldp advertise-labels interface** command to force LDP to advertise a label for a prefix constructed from an interface address and a 32-bit mask. Such a prefix is not usually in the routing table.

Examples

In the following example, the router is configured to advertise no locally assigned labels to any LDP neighbors:

```
Router(config)# no mpls ldp advertise-labels
```

In the following example, the router is configured to advertise to all LDP neighbors only the labels for networks 10.101.0.0 and 10.221.0.0:

```
Router(config)# ip access-list standard pfx-filter
Router(config-std-nacl)# permit 10.101.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.221.0.0 0.0.255.255
Router(config-std-nacl)# exit

Router(config)# mpls ldp advertise-labels for pfx-filter

Router(config)# no mpls ldp advertise-labels
```

In the following example, the router is configured to advertise the label for network 10.165.200.0 only to LSR 10.200.110.55, the label for network 10.35.35.55 only to LSR 10.150.25.25, and the labels for all other prefixes to all LSRs:

```
Router(config)# ip access-list standard pfx-filter1
Router(config-std-nacl)# permit 10.165.200.0
Router(config-std-nacl)# exit

Router(config)# ip access-list standard lsr-filter1
Router(config-std-nacl)# permit 10.200.110.55
Router(config-std-nacl)# exit

Router(config)# ip access-list standard pfx-filter2
Router(config-std-nacl)# permit 10.35.35.55
Router(config-std-nacl)# exit

Router(config)# ip access-list standard lsr-filter2
Router(config-std-nacl)# permit 10.150.25.25
Router(config-std-nacl)# exit

Router(config)# mpls ldp advertise-labels for pfx-filter1 to lsr-filter1
Router(config)# mpls ldp advertise-labels for pfx-filter2 to lsr-filter2
```

The output of the **show mpls ip binding detail** command includes the *(prefix acl, peer acl)* pairs that apply to each prefix. For this example, the applicable pairs are as follows:

```
Router# show mpls ip binding detail

Advertisement spec:
    Prefix acl = pfx-filter1; Peer acl = lsr-filter1
    Prefix acl = pfx-filter2; Peer acl = lsr-filter2

  10.35.35.55/8, rev 109
    in label:     16
        Advertised to:
        10.150.25.25:0
    out label:    imp-null  lsr: 10.200.110.55:0     inuse
    out label:    imp-null  lsr: 10.150.25.25:0
    Advert acl(s): Prefix acl pfx-filter2, Peer acl lsr-filter2
  10.165.200.0/8, rev 108
```

```
    in label:     imp-null
        Advertised to:
        10.200.110.55:0
    out label:    16        lsr: 10.200.110.55:0
    out label:    19        lsr: 10.150.25.25:0
    Advert acl(s): Prefix acl pfx-filter1, Peer acl lsr-filter1
  10.0.0.33/32, rev 98
    out label:    imp-null  lsr: 10.150.25.25:0
  10.0.0.44/32, rev 99
    in label:     imp-null
        Advertised to:
        10.200.110.55:0           10.150.25.25:0
  10.150.25.25/32, rev 101
    in label:     20
        Advertised to:
        10.200.110.55:0           10.150.25.25:0
    out label:    19        lsr: 10.200.110.55:0
    out label:    imp-null  lsr: 10.150.25.25:0     inuse
  10.0.0.44/32, rev 103
    in label:     imp-null
        Advertised to:
        10.200.110.55:0           10.150.25.25:0
    out label:    20        lsr: 10.200.110.55:0
    out label:    18        lsr: 10.150.25.25:0
  10.200.110.55/32, rev 104
    in label:     17
        Advertised to:
        10.200.110.55:0           10.150.25.25:0
    out label:    imp-null  lsr: 10.200.110.55:0     inuse
    out label:    17        lsr: 10.150.25.25:0
Router#
```

In the following example, the **vrf** keyword is specified to configure label advertisement in the VPN routing and forwarding instance named *vpn1*:

```
Router(config)# mpls ldp advertise-labels vrf vpn1 for pfx-filter1 to lsr-filter1

Router(config)# mpls ldp advertise-labels vrf vpn1 for pfx-filter2 to lsr-filter2
```

The following example uses the **interface** keyword to configure label advertisement for a /32 prefix constructed from the IP address of ethernet interface 1/1:

```
Router(config)# mpls ldp advertise-labels interface ethernet1/1
```

Related Commands

Command	Description
mpls ldp advertise-labels old-style	Uses the method of earlier software releases to interpret the **for** *prefix-access-list* parameter for the **mpls ldp advertise-labels** command.
show mpls ip binding detail	Displays detailed information about label bindings, including the access lists, if any, controlling which local labels are advertised to which LDP neighbors.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class,

mpls ldp advertise-labels old-style

To cause the **for** *prefix-access-list* parameter *of the* **mpls ldp advertise-labels** command to be interpreted according to the method used in earlier Cisco IOS software versions, use the **mpls ldp advertise-labels old-style** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp advertise-labels [**vrf** *vpn-name*] **old-style**

no mpls ldp advertise-labels [**vrf** *vpn-name*] **old-style**

Syntax Description

vrf *vpn-name*	(Optional) Specifies the VPN routing and forwarding (VRF) instance for label advertisement.

Defaults

If this command is not specified, the **for** *prefix-access-list* parameter in any **mpls ldp advertise-labels** commands is interpreted according to the rules specified under the "Usage Guidelines" section for the **mpls ldp advertise-labels** command.
If the **vrf** *vpn-name* parameter is not specified, this command applies to the default routing domain.

Command Modes

Global configuration

Command History

Release	Modification
12.0(14)ST	This command was introduced to add Multiprotocol Label Switching (MPLS) VPN support for lable distribution protocol (LDP) and to cause the **for** *prefix-access-list* parameter in the command to be interpreted in the same way as in earlier Cisco IOS releases.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The method for interpreting the for prefix-access-list parameter in the **mpls ldp advertise-labels** command is defined by Rule 2.a in the "Usage Guidelines" section in the **mpls ldp advertise-labels** command. This Rule 2.a follows normal access list conventions.

However, earlier Cisco IOS software versions used a different method for interpreting the **for** *prefix-access-list* parameter in **mpls ldp advertise-labels** command. For those earlier software versions, Rule 2.a read as follows:

2. A given prefix can have, at most, one *(prefix acl, peer acl)* pair that "applies" to it.

a. A given *(prefix acl, peer acl)* pair "applies" to a prefix only if the *prefix acl* "matches" the prefix. A match occurs if the *prefix acl* explicitly permits or denies the prefix by means of a **permit** or **deny** command. A *prefix acl* that contains a **permit any** or **deny any** command matches any prefix.

This earlier Rule 2.a departed from normal access list conventions in that:

- An explicit **deny** (including a **deny any**) that matches the prefix causes the (*prefix acl*, *peer acl*) pair to apply to the prefix.
- Explicit **deny any** and implicit **deny any** (which all access lists have) have different effects, in that the explicit **deny any** causes the access list pair to apply to all prefixes, but the implicit **deny any** has no effect.

Use the **mpls ldp advertise-labels old-style** command to force the use of the old-style method of interpreting the **for** *prefix-access-list* parameter used by earlier software versions if the following apply:

- A configuration developed for use with earlier software versions depends on this previous method for interpreting the **for** *prefix-access-list* parameter in **mpls ldp advertise-labels** commands.
- It is inconvenient to update the configuration to work with Rule 2.a as it appears under the "Usage Guidelines" section of the **mpls ldp advertise-labels** command.

Examples

The following command causes the old-style method of interpreting the **for** *prefix-access-list* parameter to be used in executing **mpls ldp advertise-labels** commands:

```
Router# mpls ldp advertise-labels old-style
```

In the following example, the **vrf** keyword is specified to configure label advertisement in the VFR instance named vpn1:

```
Router(config)# mpls ldp advertise-labels vrf vpn1 old-style
```

Related Commands

Command	Description
mpls ldp advertise-labels	Controls the distribution of locally assigned labels by means of LDP.

mpls ldp atm control-mode

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls ldp atm control-mode** command is not available in Cisco IOS software.

To control the mode used for handling label binding requests on LC-ATM interfaces, use the **mpls ldp atm control-mode** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp atm control-mode {**ordered** | **independent**}

no mpls ldp atm control-mode {**ordered** | **independent**}

Syntax Description

ordered	Delays a label binding in response to a Label Request message from a label distribution protocol (LDP) neighbor until a label binding has been received from the next hop LDP neighbor for the destination in question.
independent	Returns a label binding immediately in response to a Label Request message from an LDP neighbor. Any packets for the destination in question are discarded by the label switch router (LSR) until a label binding from the next hop LSR has been received.

Defaults

The default is **ordered** control mode.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect MPLS IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

Use of ordered control mode by an ATM device acting as a transit LSR in an ATM cloud ensures that the device will receive labeled packets to forward only after it has learned the outgoing labels required by MPLS to forward the packets. Ordered control mode relieves the device of the burden of reassembling cells into packets that must be forwarded by means of the normal (non-MPLS) packet forwarding or discard mechanisms.

Use of independent control mode on ATM transit LSRs might slightly reduce the time an ATM edge router must wait to use an ATM label switched path (LSP) it has initiated. Independent control mode eliminates the need for the edge router to wait for the Label Request/Label Mapping signaling to traverse the ATM cloud from edge router ingress to egress and back before it can send packets into the LSP. However, there is a risk that an ATM transit device might receive labeled packets before it has learned the outgoing labels required for MPLS forwarding, thus forcing the transit device to reassemble the cells into a packet that it is likely to discard.

Examples

In the following example, the mode for handling LDP Label Request messages is set to “independent” for the platform:

```
Router# mpls ldp atm control-mode independent
```

mpls ldp atm vc-merge

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls ldp atm vc-merge** command is not available in Cisco IOS software.

To control whether the vc-merge (multipoint-to-point) capability is supported for unicast label virtual circuits (LVCs), use the **mpls ldp atm vc-merge** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp atm vc-merge

no mpls ldp atm vc-merge

Syntax Description

This command has no arguments or keywords.

Defaults

The ATM-VC merge capability is enabled by default if the hardware supports this feature; otherwise, the feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect MPLS IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E and implemented on the Catalyst 6500 switch and the Cisco 7600 router.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR c.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S and implemented on the Cisco 10000(PRE-1) router.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

Use of VC merge helps conserve ATM labels by allowing incoming LSPs from different sources for the same destination to be merged onto a single outgoing VC.

Examples

In the following example, the ATM-VC merge capability is disabled:

```
Router# no mpls ldp atm vc-merge
```

Related Commands

Command	Description
show mpls atm-ldp capability	Displays the ATM MPLS capabilities negotiated with LDP neighbors for LC-ATM interfaces.

mpls ldp autoconfig

To enable Label Distribution Protocol (LDP) on interfaces for which an Open Shortest Path First (OSPF) instance or Intermediate System-to-Intermediate System (IS-IS) instance has been defined, use the **mpls ldp autoconfig** command in **router** configuration mode. To disable this feature, use the **no** form of this command.

For OSPF

mpls ldp autoconfig [**area** *area-id*]

no mpls ldp autoconfig [**area** *area-id*]

For IS-IS

mpls ldp autoconfig [*level-1* | *level-2*]

no mpls ldp autoconfig

Syntax Description

area *area-id*	(Optional) Enables LDP on the interfaces belonging to the specified OSPF area.
level-1 | *level-2*	(Optional) Enables LDP for a specified IS-IS level. If an interface is enabled for the same level as autoconfiguration, then LDP is enabled over that interface. If the interface has a different level than autoconfiguration, LDP is not enabled. By default, without the use of these arguments, the configuration is applied to both the levels.

Defaults

LDP is not enabled on interfaces. If an OSPF area or an IS-IS level is not specified, LDP is enabled on all interfaces belonging to the OSPF or IS-IS process.

Command Modes

Router configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.0(32)SY	This command was modified to support IS-IS processes in Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

- You can specify this command multiple times to enable LDP on different routing areas with interfaces running OSPF.
- If LDP is disabled globally, the **mpls ldp autoconfig** command fails. LDP must be enabled globally by means of the global **mpls ip** command first.
- If the **mpls ldp autoconfig** command is configured, you cannot issue the global **no mpls ip** command. If you want to disable LDP, you must issue the **no mpls ldp autoconfig** command first.
- The **mpls ldp autoconfig** command is supported only with OSPF and IS-IS interior gateway protocols (IGPs).
- The MPLS LDP Autoconfiguration feature supports IS-IS only in Cisco IOS Release 12.0(32)SY.
- 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.
- For IS-IS interfaces, the level for which an interface is configured must be compatible with the level for which autoconfiguration is desired.
- For IS-IS interfaces, each application of the configuration command overwrites the earlier configuration. If initial autoconfiguration is enabled for level-1 and a later configuration specifies level-2, LDP is enabled only on IS-IS level-2 interfaces.

Examples

In the following example, MPLS LDP Autoconfiguration is enabled for OSPF area 5:

```
Router(config-router)# mpls ldp autoconfig area 5
```

Related Commands

Command	Description
mpls ldp igp autoconfig	Enables LDP on an interface.
show mpls interfaces	Displays information about interfaces configured for LDP.
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp backoff

To configure parameters for the label distribution protocol (LDP) backoff mechanism, use the **mpls ldp backoff** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp backoff *initial-backoff maximum-backoff*

no mpls ldp backoff *initial-backoff maximum-backoff*

Syntax Description

initial-backoff	Number from 5 to 2147483, inclusive, that defines the initial backoff value in seconds. The default is 15 seconds.
maximum-backoff	Number from 5 to 2147483, inclusive, that defines the maximum backoff value in seconds. The default value is 120 seconds.

Defaults

The initial backoff value is 15 seconds and grows to a maximum value of 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was implemented on the Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR card.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The LDP backoff mechanism prevents two incompatibly configured label switch routers (LSRs) from engaging in an unthrottled sequence of session setup failures. For example, an incompatibility arises when two neighboring routers attempt to perform LC-ATM (label-controlled ATM) but the two are using different ranges of VPI/VCI values for labels.

If a session setup attempt fails due to an incompatibility, each LSR delays its next attempt (that is, backs off), increasing the delay exponentially with each successive failure until the maximum backoff delay is reached.

The default settings correspond to the lowest settings for initial and maximum backoff values defined by the LDP protocol specification. You should change the settings from the default values only if such settings result in undesirable behavior.

Examples

The following command shows how to set the initial backoff delay to 30 seconds and the maximum backoff delay to 240 seconds:

```
Router(config)# mpls ldp backoff 30 240
```

Related Commands

Command	Description
show mpls ldp backoff	Displays information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp discovery

To configure the interval between transmission of consecutive Label Distribution Protocol (LDP) discovery hello messages, or the hold time for a discovered LDP neighbor, or the neighbors from which requests for targeted hello messages may be honored, use the **mpls ldp discovery** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp discovery {**hello** {**holdtime** | **interval**} *seconds* | **targeted-hello** {**holdtime** | **interval**} *seconds* | **accept** [**from** *acl*]}

no mpls ldp discovery {**hello** {**holdtime** | **interval**} | **targeted-hello** {**holdtime** | **interval**} | **accept** [**from** *acl*]}

Syntax Description

hello	Configures the intervals and hold times for directly connected neighbors.
holdtime	Defines the period of time a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor. The default value for the **holdtime** keyword is 15 seconds for link hello messages and 90 seconds for targeted hello messages.
interval	Defines the period of time between the sending of consecutive hello messages. The default value for the **interval** keyword is 5 seconds for link hello messages and 10 seconds for targeted hello messages.
seconds	Hold time or interval in seconds: • The default hold time is 15 seconds for link hello messages and 90 seconds for targeted hello messages. • The default interval is 5 seconds for link hello messages and 10 seconds for targeted hello messages.
targeted-hello	Configures the intervals and hold times for neighbors that are not directly connected (for example, LDP sessions that run between the endpoints of an LSP tunnel).
accept	Configures the router to respond to requests for targeted hello messages from all neighbors or from neighbors specified by the optional *acl* argument.
from *acl*	(Optional) The IP access list that specifies the neighbor from which requests for targeted hello messages may be honored.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) IETF command syntax and terminology.

Release	Modification
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. Default values for the **holdtime** and **interval** keywords were changed.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

The discovery hold time is set to the smaller of the following: the locally proposed hold time or the hold time proposed by the neighbor. The hello interval is selected so that within the hello hold time period at least three hellos messages are sent for a link hello and at least nine hello messages are sent for a targeted hello.

When the discovery hold time elapses for a neighbor discovered on an interface or for a neighbor discovered by means of a targeted hello message, the record associating the neighbor with that interface or the targeted hello message source is discarded. If an LDP session exists with a neighbor, but a discovery record no longer exists for that neighbor, the LDP session is terminated.

Setting the hold time too high causes LDP to be slow in detecting link outages; setting the hold time too low might cause LDP to terminate sessions when a hello message is dropped during traffic bursts on a link.

The exchange of targeted hello messages between two nondirectly connected neighbors (N1 and N2) may occur in the following ways:

- N1 may initiate the transmission of targeted hello messages to N2, and N2 may send targeted hello messages in response. In this situation, N1 is considered to be active and N2 is considered to be passive.

  N1 targeted hello messages carry a request that N2 send targeted hello messages in response. To respond, N2 configuration must permit it to respond to N1. The **mpls ldp discovery targeted-hello accept** command is used to configure whether N1 must respond to requests for targeted hello messages.

- Both N1 and N2 may be configured to initiate the transmission of targeted hello messages to each other. In this situation, both are active.

  Both, one, or neither of N1 and N2 may be passive, depending on whether they have been configured to respond to requests for targeted hello messages from the other.

Note Normally, active transmission of targeted hello messages on a router is triggered by some configuration action, such as an **mpls ip** command on a traffic engineering tunnel interface.

Examples

The following example shows how to set the period of time to 30 seconds for which a neighbor discovered on an interface is remembered, if no hello messages are received:

```
Router# configure terminal
Router(config)# mpls ldp discovery hello holdtime 30
```

The following example shows how to configure the router to respond to requests for targeted hello messages from neighbors 209.165.200.225 and 209.165.200.234:

```
Router(config)# ip access standard TRGT-ACCEPT
Router(config-nacl)# permit 209.165.200.225
Router(config-nacl)# permit 209.165.200.234
Router(config-nacl)# exit
Router(config)# mpls ldp discovery targeted-hello from TRGT-ACCEPT
```

Related Commands

Command	Description
mpls ip	Enables MPLS forwarding of IPv4 packets along normally routed paths.
mpls ldp holdtime	Changes the time for which an LDP session is maintained in the absence of LDP messages from the session peer.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp discovery transport-address

To specify the transport address advertised in the Label Distribution Protocol (LDP) discovery hello messages sent on an interface, use the **mpls ldp discovery transport-address** command in interface configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp discovery transport-address {**interface** | *IP-address*}

no mpls ldp discovery transport-address

Syntax Description

interface	Specifies that the interface IP address should be advertised as the transport address.
IP-address	IP address advertised as the transport address.

Command Default

The default behavior when this command has not been issued for an interface depends on the interface type.
Unless the interface is a label-controlled ATM (LC-ATM) interface, LDP advertises its LDP router ID as the transport address in LDP discovery hello messages sent from the interface.
If the interface is an LC-ATM interface, no transport address is explicitly advertised in LDP discovery hello messages sent from the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

The establishment of an LDP session between two routers requires a session TCP connection by which label advertisements can be exchanged between the routers. To establish the session TCP connection, each router must know the transport address (IP address) of the other router.

The LDP discovery mechanism provides the means for a router to advertise the transport address for its end-of-session TCP connection. When the transport address advertisement is explicit, the transport address appears as part of the contents of discovery hello messages sent to the peer. When the transport address advertisement is implicit, the transport address is not included in the discovery hello messages, and the peer uses the source IP address of received hello messages as the peer transport address.

The **mpls ldp discovery transport-address** command provides the means to modify the default behavior described in the Command Default section of this document. When the **interface** keyword is specified, LDP advertises the IP address of the interface in LDP discovery hello messages sent from the interface. When the *IP-address* argument is specified, LDP advertises the specified IP address in LDP discovery hello messages sent from the interface.

Note When a router has multiple links connecting it to its peer device, the router must advertise the same transport address in the LDP discovery hello messages it sends on all such interfaces.

Examples

The following example shows how to specify the LDP transport address for interface pos2/0 should be the interface IP address; it also shows how to specify the IP address 209.165.200.225 of interface pos3/1 should be the LDP transport address:

```
Router(config#) interface pos2/0
Router(config-if)# mpls ldp discovery transport-address interface
Router(config#) interface pos3/1
Router(config-if)# mpls ldp discovery transport-address 209.165.200.225
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.

mpls ldp explicit-null

To cause a router to advertise an Explicit Null label in situations where it would normally advertise an Implicit Null label, use the **mpls ldp explicit-null** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp explicit-null [**for** *prefix-acl* | **to** *peer-acl* | **for** *prefix-acl* **to** *peer-acl*]

no mpls ldp explicit-null

Syntax Description

for *prefix-acl*	(Optional) Specifies prefixes for which Explicit Null should be advertised in place of Implicit Null.
to *peer-acl*	(Optional) Specifies Label Distribution Protocol (LDP) peers to which Explicit Null should be advertised in place of Implicit Null.

Defaults

Implicit Null is advertised for directly connected routes unless the command **mpls ldp explicit-null** has been executed.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the previous hop (penultimate) router to do penultimate hop popping. Situations exist where it might be desirable to prevent the penultimate router from performing penultimate hop popping and to force it to replace the incoming label with the Explicit Null label.

When you issue the **mpls ldp explicit-null** command, Explicit Null is advertised in place of Implicit Null for directly connected prefixes permitted by the *prefix-acl* argument to peers permitted by the *peer-acl argument*.

If you do not specify the *prefix-acl* argument in the command, Explicit Null is advertised in place of Implicit Null for all directly connected prefixes.

If you do not specify the *peer-acl* argument in the command, Explicit Null is advertised in place of Implicit Null to all peers.

Examples

The following command shows how to cause Explicit Null to be advertised for all directly connected routes to all LDP peers:

```
Router(config)# mpls ldp explicit-null
```

The following command sequence shows how to cause Explicit Null to be advertised for directly connected route 10.5.0.0 to all LDP peers and Implicit Null to be advertised for all other directly connected routes:

```
Router(config)# mpls ldp explicit-null
Router(config)# ip access-list standard adv-exp-null
Router(config-std-nacl)# permit 10.5.0.0
Router(config-std-nacl)# deny any
Router(config-std-nacl)#
```

Related Commands

Command	Description
show mpls ip binding	Displays specified information about label bindings learned by LDP.

mpls ldp graceful-restart

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Graceful Restart, use the **mpls ldp graceful-restart** command in global configuration mode. To disable LDP Graceful Restart, use the **no** form of this command.

mpls ldp graceful-restart

no mpls ldp graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

LDP Graceful Restart is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

LDP Graceful Restart must be enabled before an LDP session is established.

Using the **no** form of the command disables the Graceful Restart functionality on all LDP sessions.

Examples

The command in the following example enables LDP Graceful Restart on a router:

```
Router(config)# mpls ldp graceful-restart
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers forwarding-holding

To specify the amount of time the Multiprotocol Label Switching (MPLS) forwarding state should be preserved after the control plane restarts, use the **mpls ldp graceful-restart timers forwarding-holding** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers forwarding-holding *secs*

no mpls ldp graceful-restart timers forwarding-holding

Syntax Description

secs	The amount of time (in seconds) that the MPLS forwarding state should be preserved after the control plane restarts. The default is 600 seconds. The acceptable range of values is 30 to 600 seconds.

Command Default

After the control plane on the Cisco 7500 and Cisco 10000 series router restarts, the MPLS forwarding state is preserved for 600 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Configuring the local forwarding-holding timer to a value less than the IOS FT Reconnect Timeout of 120 seconds may prevent a Label Distribution Protocol (LDP) session from being established. Configure the forwarding-holding timer to less than 120 seconds only if an LDP neighbor has an FT Reconnect Timeout value of less than 120 seconds.

If the timer expires, all entries that are marked stale are deleted.

Examples

In the following example, the MPLS forwarding state is preserved for 300 seconds after the control plane restarts:

```
Router(config)# mpls ldp graceful-restart timers forwarding-holding 300
```

Related Commands

Command	Description
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers max-recovery

To specify the amount of time a router should hold stale label-Forwarding Equivalence Class (FEC) bindings after a Label Distribution Protocol (LDP) session has been reestablished, use the **mpls ldp graceful-restart timers max-recovery** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers max-recovery *secs*

no mpls ldp graceful-restart timers max-recovery

Syntax Description

secs	The amount of time (in seconds) that the router should hold stale label-FEC bindings after an LDP session has been reestablished. The default is 120 seconds. The acceptable range of values is 15 to 600 seconds.

Command Default

Stale label-FEC bindings are held for 120 seconds after an LDP session has been reestablished.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

After the timer expires, all stale label-FEC bindings learned from the associated LDP session are removed, which results in the removal of any forwarding table entries that are based on those bindings.

Examples

In the following example, the router should hold stale label-FEC bindings after an LDP session has been reestablished for 180 seconds:

```
Router(config)# mpls ldp graceful-restart timers max-recovery 180
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers neighbor-liveness	Specifies the amount of time a router should wait for an LDP session to be reestablished.

mpls ldp graceful-restart timers neighbor-liveness

To specify the upper bound on the amount of time a router should wait for a Label Distribution Protocol (LDP) session to be reestablished, use the **mpls ldp graceful-restart timers neighbor-liveness** command in global configuration mode. To revert to the default timer value, use the **no** form of this command.

mpls ldp graceful-restart timers neighbor-liveness *secs*

no mpls ldp graceful-restart timers neighbor-liveness

Syntax Description

secs	The amount of time (in seconds) that the router should wait for an LDP session to be reestablished. The default is 120 seconds. The range is 5 to 300 seconds.

Command Default

The default is a maximum of 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The amount of time a router waits for an LDP session to be reestablished is the lesser of the following values:

- The value of the peer's fault tolerant (FT) type length value (TLV) reconnect timeout
- The value of the neighbor liveness timer

If the router cannot reestablish an LDP session with the neighbor in the time allotted, the router deletes the stale label-FEC bindings received from that neighbor.

Examples

The command in the following example sets the amount of time that the router should wait for an LDP session to be reestablished to 30 seconds:

```
Router(config)# mpls ldp graceful-restart timers neighbor-liveness 30
```

Related Commands

Command	Description
mpls ldp graceful-restart timers forwarding-holding	Specifies the amount of time the MPLS forwarding state should be preserved after the control plane restarts.
mpls ldp graceful-restart timers max-recovery	Specifies the amount of time a router should hold stale label-FEC bindings after an LDP session has been reestablished.

mpls ldp holdtime

To change the time for which an Label Distribution Protocol (LDP) session is maintained in the absence of LDP messages from the session peer, use the **mpls ldp holdtime** command in global configuration mode. To disable this command, use the **no** form of the command.

mpls ldp holdtime *seconds*

no mpls ldp holdtime *seconds*

Syntax Description

seconds	Number from 15 to 2147483 that defines the time, in seconds, an LDP session is maintained in the absence of LDP messages from the session peer. The default is 180.

Defaults

The default value for the *seconds* argument is 180.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Swithcing (MPLS) IETF command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)s	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an LDP session is established between two LSRs, the hold time used for the session is the lower of the values configured on the two LSRs.

Examples

The following example shows how to configure the hold time of LDP sessions for 30 seconds:

```
Router# mpls ldp holdtime 30
```

Related Commands

Command	Description
show mpls ldp parameters	Displays the current LDP parameter.
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.

mpls ldp igp autoconfig

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) autoconfiguration on an interface that belongs to an Open Shortest Path First (OSPF) area, use the **mpls ldp igp autoconfig** command in interface configuration mode. To disable MPLS LDP autoconfiguration, use the **no** form of the command.

mpls ldp igp autoconfig

no mpls ldp igp autoconfig

Syntax Description

This command has no arguments or keywords.

Command Default

This command works with the **mpls ldp autoconfig** command, which enables LDP on all interfaces that belong to an OSPF area. So, by default, all interfaces are enabled for LDP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

This command works with the **mpls ldp autoconfig** command, which enables LDP on all interfaces that belong to an OSPF area. To disable LDP on selected interfaces, use the **no mpls ldp igp autoconfig** command.

Examples

The following example shows how to disable LDP on interface POS1/0:

```
Router(config)# interface pos1/0
Router(config-if)# no mpls ldp igp autoconfig
```

Related Commands

Command	Description
mpls ldp autoconfig	Globally enables LDP on all interfaces that belong to an OSPF area.
show mpls interfaces	Displays information about interfaces configured for LDP.
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp igp sync

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization on an interface that belongs to an Open Shortest Path First (OSPF) process, use the **mpls ldp igp sync** command in interface configuration mode. To disable MPLS LDP-IGP synchronization, use the **no** form of the command.

mpls ldp igp sync [**delay** *seconds*]

no mpls ldp igp sync [**delay**]

Syntax Description

delay	(Optional) Sets a delay timer for MPLS LDP-IGP synchronization.
seconds	(Optional) Delay time, in seconds. The range is from 5 to 60 seconds.

Command Default

If MPLS LDP-IGP synchronization is enabled on an OSPF process, MPLS LDP-IGP synchronization is enabled by deffault on all interfaces configured for the process. A delay timer is not set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.0(32)S	The optional **delay** *seconds* keyword and argument were added.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

This command works with the **mpls ldp sync** command, which enables MPLS LDP-IGP synchronization on all interfaces that belong to an OSPF process. To disable MPLS LDP-IGP synchronization on a selected interface, use the **no mpls ldp igp sync** command in the configuration for that interface.

Use the **mpls ldp igp sync delay** *seconds* command to configure a delay time for MPLS LDP and IGP synchronization on an interface-by-interface basis. To remove the delay timer from a specified interface, use the **no mpls ldp igp sync delay** command. This command sets the delay time to 0 seconds, but leaves MPLS LDP-IGP synchronization enabled.

When LDP is fully established and synchronized, LDP checks the delay timer:

- If you configured a delay time, LDP starts the timer. When the timer expires, LDP checks that synchronization is still valid and notifies the OSPF process.
- If the delay time is not configured, synchronization is disabled or down, or an interface is removed from an IGP process, LDP stops the timer and immediately notifies the OSPF process.

If you configure a new delay time while a timer is running, LDP saves the new delay time but does not reconfigure the running timer.

Examples

The following example shows how to disable MPLS LDP-IGP synchronization on POS interface 1/0:

```
Router(config)# interface pos1/0
Router(config-if)# no mpls ldp igp sync
```

The following example shows how to set a delay timer of 45 seconds for MPLS LDP-IGP synchronization on FastEthernet interface 0/0:

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# mpls ldp igp sync delay 45
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp igp sync holddown

To specify how long an Interior Gateway Protocol (IGP) should wait for Label Distribution Protocol (LDP) synchronization to be achieved, use the **mpls ldp igp sync holddown** command in global configuration mode. To disable the hold-down timer, use the **no** form of this command.

mpls ldp igp sync holddown *milliseconds*

no mpls ldp igp sync holddown

Syntax Description

milliseconds	The number of milliseconds an IGP should wait for an LDP session to be established. The valid range of values is 1 to 2147483647.

Command Default

An IGP will wait indefinitely for LDP synchronization to be achieved.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command enables you to limit the amount of time an IGP waits for LDP synchronization to be achieved.

Examples

In the following example, the IGP is limited to 10,000 milliseconds (10 seconds):

```
Router(config)# mpls ldp igp sync holddown 10000
```

Related Commands

Command	Description
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp label

To enter MPLS LDP label configuration mode to specify how Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) handles local label allocation, use the **mpls ldp label** command in global configuration mode. To remove all local label allocation filters configured in MPLS LDP label configuration mode and restore LDP default behavior for local label allocation without a session reset, use the **no** form of this command.

mpls ldp label

no mpls ldp label

Syntax Description

This command has no arguments or keywords.

Command Default

LDP label configuration mode commands are not available.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

After you enter the **mpls ldp label** command, you can specify a prefix list or host routes to filter prefixes for MPLS LDP local label allocation.

Use the **no** form of the command to remove prefix filtering for local label allocation and restore the default LDP local allocation behavior without resetting the session.

A maximum of one filter configuration is allowed for the global table.

Examples

The following example shows how to enter MPLS LDP label configuration mode, specify the prefix list named list1 to filter prefixes for MPLS LDP local label allocation, and exit MPLS LDP label configuration mode:

```
configure terminal
!
mpls ldp label
 allocate global prefix-list list1
 exit
```

The following examples shows how to remove all local label allocation filters in MPLS LDP label configuration mode and restore LDP default behavior for local label allocation:

```
configure terminal
!
no mpls ldp label
```

Related Commands

Command	Description
allocate	Configures local label allocation filters for learned routes for MPLS LDP.

mpls ldp logging neighbor-changes

To generate system error logging (syslog) messages when Label Distribution Protocol (LDP) sessions go down, use the **mpls ldp logging neighbor-changes** command in global configuration mode. To disable generating syslog messages, use the **no** form of this command.

mpls ldp logging neighbor-changes

no mpls ldp logging neighbor-changes

Syntax Description

This command has no arguments or keywords.

Defaults

Logging is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)T	This command was integrated into Cisco IOS Release 12.2(14)T.
12.0(31)S	The log message is updated to show a VPN routing/forwarding instance (VRF) information and the reason for an LDP neighbor going down.
12.3(15)	The log message is updated to show VRF information and the reason for an LDP neighbor going down.
12.4(1)	The log message is updated to show VRF information and the reason for an LDP neighbor going down.
12.2(28)S	The log message is updated to show VRF information and the reason for an LDP neighbor going down.

Usage Guidelines

Use the **mpls ldp logging neighbor-changes** command to generate syslog messages when an LDP session goes down. The command also provides VRF information about the LDP neighbor and the reason for the LDP session going down. Some of the reasons for an LDP session going down are the following:

- An LDP was disabled globally by configuration.
- An LDP was disabled on an interface.

Examples

The following example generates syslog messages when LDP sessions go down:

Router(config)# **mpls ldp logging neighbor-changes**

The following output shows the log entries when an LDP session with neighbor 192.168.1.100:0 goes down and comes up. The session went down because the discovery hold timer expired. The VRF table identifier for the neighbor is 1.

```
2d00h: %LDP-5-NBRCHG: LDP Neighbor 192.168.1.100:0 (1) is DOWN (Disc hold timer expired)
2d00h: %LDP-5-NBRCHG: LDP Neighbor 192.168.1.100:0 (1) is UP
```

mpls ldp logging password configuration

To enable the display password configuration change events on an MPLS Label Switch Router (LSR), use the **mpls ldp logging password configuration** command in global configuration mode. To disable the display of password events, use the **no** form of this command.

mpls ldp logging password configuration [**rate-limit** *num*]

no mpls ldp logging password configuration

Syntax Description

rate-limit *num*	(Optional) Specifies a rate limit of 1 to 60 messages per minute.

Defaults

Logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The logging output displays events when a new password is configured or an existing password has been changed or deleted.

Related Commands

Command	Description
mpls ldp logging password rollover	Enables the display password rollover events on an MPLS LSR.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.

Command	Description
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp logging password rollover

To enable the display password rollover events on an MPLS Label Switch Router (LSR), use the **mpls ldp logging password rollover** command in global configuration mode. To disable the display of password events, use the **no** form of this command.

mpls ldp logging password rollover [**rate-limit** *num*]

no mpls ldp logging password rollover

Syntax Description

rate-limit *num*	(Optional) Specifies a rate limit of 1 to 60 messages per minute.

Defaults

Logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The logging output displays events when a new password is used for authentication or when authentication is disabled.

Related Commands

Command	Description
mpls ldp logging password configuration	Enables the display password configuration change events on an MPLS LSR.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.

Command	Description
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp loop-detection

To enable the label distribution protocol (LDP) optional loop detection mechanism, use the **mpls ldp loop-detection** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp loop-detection

no mpls ldp loop-detection

Syntax Description

This command has no optional keywords or arguments.

Defaults

LDP loop detection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The LDP loop detection mechanism is intended for use in networks of devices that do not use time-to-live mechanisms (for example, ATM switches) that cannot fairly allocate device resources among traffic flows.

The LDP loop detection mechanism is used with the Downstream on Demand method of label distribution, supplementing the Downstream on Demand hop count mechanism to detect looping LSPs that might occur during routing transitions.

Examples

The following command sets the LDP loop detection mechanism on:

```
Router(config)# mpls ldp loop-detection
```

Related Commands

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.

mpls ldp maxhops

To limit the number of hops permitted in a label switched path (LSP) established by the Downstream on Demand method of label distribution, use the **mpls ldp maxhops** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp maxhops *number*

no mpls ldp maxhops

Syntax Description

number	Number from 1 to 255, inclusive, that defines the maximum hop count. The default is 254.

Defaults

The default is 254 hops.

Command Modes

Global configuration

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was updated with MPLS command syntax and terminology.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an ATM label switch router (LSR) initiates a request for a label binding, it sets the hop count value in the Label Request message to 1. Subsequent ATM-LSRs along the path to the edge of the ATM label switching region increment the hop count before forwarding the Label Request message to the next hop.

When an ATM LSR receives a Label Request message, it does not send a Label Mapping message in response, nor does it propagate the request to the destination next hop if the hop count value in the request equals or exceeds the maxhops value. Instead, the ATM LSR returns an error message that specifies that the maximum allowable hop count has been reached. This threshold is used to prevent forwarding loops in the setting up of label switch paths across an ATM region.

Examples

The following example sets the hop count limit to 10:

```
Router(config)# mpls ldp maxhops 10
```

Related Commands

Command	Description
mpls ldp router-id	Specifies a preferred interface for determining the LDP router ID.
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.
show mpls ip binding	Displays specified information about label bindings learned by LDP.

mpls ldp neighbor implicit-withdraw

To configure the advertisement of a new label for a Forwarding Equivalence Class (FEC) without the withdrawal of the previously advertised label, use the **mpls ldp neighbor implicit-withdraw** command in global configuration mode. To disable this option for the specified neighbor, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* **implicit-withdraw**

no mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* [**implicit-withdraw**]

Syntax Description

vrf *vpn-name*	(Optional) VPN routing and forwarding instance for the specified neighbor.
ip-addr	Router ID (IP address) that identifies a neighbor.

Defaults

When the **vrf** keyword is not specified in this command, the label distribution protocol (LDP) neighbor is configured in the default routing domain.

If this command is not configured, when it is necessary for LDP to change the label it has advertised to a neighbor for some prefix, it will withdraw the previously advertised label before advertising the new label to the neighbor.

For the **no** form of the command, if the **implicit-withdraw** keyword is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)ST	This command was modified to add the **implicit-withdraw** keyword.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was implemented on the Cisco 10000(PRE-1) router.
12.2(13)T	This command was implemented on the Cisco 2600 and 3600 routers.
12.2(14)S	This command was implemented on the Cisco 7200 and 7500 series routers and integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, in Cisco IOS Release 12.0(21)ST and later, LDP withdraws the previously advertised label by using a withdraw message before advertising a new label for a FEC. In Cisco IOS releases prior to 12.0(21)ST, LDP did not withdraw a previously advertised label before advertising a new label for a FEC. In those older releases, the new label advertisement served as an implied withdraw and LDP did not send a withdraw message. To cause LDP now to operate as it did in releases before Cisco IOS release 12.0(21)ST—that is, to make LDP now advertise a new label for a FEC without first withdrawing the previously advertised label—use this command's **implicit-withdraw** keyword.

```
Router(config)# mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Using the **implicit-withdraw** keyword avoids generating the overhead from an exchange of label withdraw and label release messages.

To disable the **implicit-withdraw** option, use the **no** form of the command with the **implicit-withdraw** keyword. This returns the router to the default, which requires that LDP withdraw the previously advertised label for a FEC before advertising a new label.

```
Router(config)# no mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Examples

In the following example, LDP does not send a label-withdraw message to the neighbor whose router ID is 10.10.10.10 when a need exists to change the previously advertised label for a FEC:

```
Router(config)# mpls ldp neighbor 10.10.10.10 implicit-withdraw
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp neighbor targeted	Sets up a targeted session with the specified neighbor.

mpls ldp neighbor labels accept

To configure a label switching router (LSR) to filter label distribution protocol (LDP) inbound label bindings from a particular LDP peer, use the **mpls ldp neighbor labels accept** command in **global** configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl*

no mpls ldp neighbor [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl*

Syntax Description

vrf *vpn-name*	(Optional) Specifies VPN routing and forwarding instance (*vpn-name*) for accepting labels.
nbr-address	Specifies address of the LDP peer whose advertisements are to be filtered.
labels accept *acl*	Specifies the prefixes (access control list) that are acceptable (permitted).

Defaults

If the **vrf** keyword is not specified, the specified LDP neighbor is configured in the default routing domain.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The specified ACL is used to filter label bindings advertised by the specified neighbor. If the prefix part of the label binding is permitted by the ACL, the router will accept the binding. If the prefix is denied, the router will not accept or store the binding.

This functionality is particularly useful when two different entities manage peer LSRs; that is, the recipient cannot perform filtering by altering the configuration of the sender. This is likely to occur in an Multiprotocol Label Switching (MPLS) virtual private network (VPN) that is using the LDP-based Carrier Supporting Carrier (CSC) feature. In that situation, the backbone carrier may want to restrict the set of label bindings that its provider edge (PE) router may learn from an adjacent customer edge (CE) router that a customer carrier operates.

When inbound label binding filtering is configured, certain configuration changes may require a router to retain bindings that it previously discarded. For example:

- Inbound filtering is disabled.
- An inbound filtering ACL is redefined to be less restrictive.

A router does not maintain a record of the set of bindings it previously discarded. Therefore, it cannot ask its neighbors to readvertise just those bindings. In addition, LDP (as defined by RFC 3036) does not provide a means for a router to signal its neighbors to readvertise all label bindings. Consequently, to relearn label bindings following such configuration changes, you must reset the LDP session or sessions by using the **clear mpls ldp neighbor** command.

Note The **mpls ldp neighbor labels accept** command has no effect on an LC-ATM interface. Such an interface behaves as though this command had not been executed. The **mpls ldp request-labels** ACL command, which is supported for LC-ATM, controls which label bindings are requested (accepted) from neighbors.

Examples

The following example specifies that the LSR accepts inbound label bindings from neighbor 10.19.19.19 in vrf vpn1 for prefixes permitted by the ACL named aclone:

```
Router(config)# mpls ldp neighbor vrf vpn1 10.19.19.19 label accept aclone
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
mpls ldp advertise-labels	Controls the distribution of locally assigned (incoming) labels by means of LDP.
show ip access list	Displays the list of configured access lists and their definitions.
show mpls ldp neighbor	Displays the status of the LDP sessions.

mpls ldp neighbor password

To configure a password for computing message digest algorithm 5 (MD5) checksums for the session TCP connection with the specified neighbor, use the **mpls ldp neighbor password** command in global configuration mode. To disable this option for the specified neighbor, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *ip-address* **password** *password*

no mpls ldp neighbor [**vrf** *vpn-name*] *ip-address* [**password** *password*]

Syntax Description

vrf *vpn-name*	(Optional) VPN routing and forwarding instance for the specified neighbor.
ip-address	Router ID (IP address) that identifies a neighbor.
password	Password used for computing MD5 checksums for the session TCP connection with the specified neighbor.

Defaults

Unless the TCP MD5 Signature Option is explicitly configured with the password for session TCP connections, the option is not used.
When the **vrf** name is not specified in this command, the Label Distribution Protocol (LDP) neighbor is configured in the default routing domain.
For the **no** form of the command, if the password is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	This command was integrated in Cisco IOS Release 12.0(33)S.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You can invoke authentication between two LDP peers, verifying each segment sent on the TCP connection between the peers. To do so, you must configure authentication on both LDP peers using the same password; otherwise, the peer session is not established.

The authentication capability uses the MD5 algorithm. MD5, an algorithm used in conjunction with SNMP, verifies the integrity of the communication, authenticates the origin of the message, and checks for timeliness.

Invoking the **mpls ldp neighbor password** command causes the generation and checking of the MD5 digest for every segment sent on the TCP connection.

Configuring a password for an LDP neighbor causes an existing LDP session to be torn down and a new session to be established.

If a router has a password configured for a neighbor, but the neighbor router does not have a password configured, a message such as the following appears on the console while the two routers attempt to establish an LDP session:

```
%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:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:646
```

Examples

In the following example, the password (password1) is configured as the password for use with MD5 for the neighbor whose router ID is 139.27.0.15:

```
Router(config)# mpls ldp neighbor 139.27.0.15 password password1
```

In the following example, the password (password1) is configured as the password for use with MD5 for the LDP neighbor having router ID 4.4.4.4 in the VPN routing and forwarding instance named vpn1:

```
Router(config)# mpls ldp neighbor vrf vpn1 4.4.4.4 password password1
```

Related Commands

Command	Description
mpls ldp neighbor implicit-widthdraw	Configures the advertisement of a new label for a FEC without the withdrawal of the previously advertised label.
mpls ldp neighbor targeted	Sets up a targeted session with the specified neighbor.

mpls ldp neighbor targeted

To set up a targeted session with a specified neighbor, use the **mpls ldp neighbor targeted** command in global configuration mode. To disable a targeted session, use the **no** form of this command.

mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* **targeted** [**ldp** | **tdp**]

no mpls ldp neighbor [**vrf** *vpn-name*] *ip-addr* [**targeted** [**ldp** | **tdp**]]

Syntax Description

vrf *vpn-name*	(Optional) VPN routing and forwarding (VRF) instance for a specified neighbor.
ip-addr	Router ID (IP address) that identifies a neighbor.
ldp	(Optional) Specifies Label Distribution Protocol (LDP) as the label protocol for the targeted session.
tdp	(Optional) Specifies Tag Distribution Protocol (TDP) as the label protocol for the targeted session.

Defaults

When the **targeted** keyword is not specified, a targeted session is not set up with the neighbor. For the **no** form of the command, if the **targeted** keyword is not specified, all configuration information for the specified neighbor reverts to the defaults and the neighbor record is deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify the label protocol for the targeted session, the label protocol specified with the **mpls label protocol** command is used. If the **mpls label protocol** command is not configured, then LDP is used for the targeted session.

Use the **mpls ldp neighbor targeted** command when you need to set up a targeted session and 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 would use this command to set up 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 links 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.

Examples

In the following example, the router sets up a targeted session with the neighbor 10.10.10.10 using TDP as the label protocol:

```
Router(config)# mpls ldp neighbor 10.10.10.10 targeted
```

In the following example, the router sets up a targeted session with the neighbor 10.10.10.10 using LDP as the label protocol:

```
Router(config)# mpls label protocol ldp

Router(config)# mpls ldp neighbor 10.10.10.10 targeted
```

Another way to set up a targeted session using LDP without changing the default label protocol is as follows:

```
Router(config)# mpls ldp neighbor 10.10.10.10 targeted ldp
```

Related Commands

Commands	Description
mpls ldp neighbor implicit-widthdraw	Configures the advertisement of a new label for a FEC without the withdrawal of the previously advertised label.
mpls ldp neighbor password	Configure a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.

mpls ldp password fallback

To configure a message digest algorithm 5 (MD5) password for Label Distribution Protocol (LDP) sessions with peers, use the **mpls ldp password fallback** command in global configuration mode. To remove the MD5 password, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password fallback** {**key-chain** *keychain-name* | [**0** | **7**] *password*}

no mpls ldp [**vrf** *vrf-name*] **password fallback**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
key-chain *keychain-name*	(Optional) Specifies the name of the key chain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic.
0 | **7**	(Optional) Specifies whether the *password* that follows is encrypted: • **0** specifies an unencrypted password. • **7** specifies an encrypted password.
password	Specifies the MD5 password to be used for the LDP sessions with peers whose connections are established through a named VRF or the global routing table.

Defaults

The MD5 password for LDP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.0(33)S	The **key-chain** *keychian-name* keyword-argument pair argument was added.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the default password for the VRF routing table. The VRF routing table name is specified by the *vrf-name* argument when you configure the **vrf** keyword for the command. If you do not include the **vrf** keyword in the command, the command specifies the default password for the global routing table. The password configured by this command is the password used for sessions between peers, if neither of the following commands applies: the **mpls ldp neighbor password** command or the **mpls ldp password option** command.

If you configure a type 7 (encrypted) password, the password is saved in encrypted form.

If you configure a type 0 (clear-text) password, it can be saved in clear-text form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, then the type 0 password is converted and saved in encrypted form.
- If the **service password-encryption** command is disabled, then the type 0 password is saved in clear-text (nonencrypted) form.

When you enter a **show running-config** command, if the global **service password-encryption** command is enabled, a password saved in clear-text form is converted into encrypted form, and displayed and saved in encrypted form.

Examples

The following example shows how to configure an MD5 password for an LDP session with peers in VRF vpn1:

```
Router> enable
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls ldp vrf vpn1 password fallback secure
Router(config)# exit
Router#
```

The password, secure, would be encrypted. It is shown here as you would enter it on the command line.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password option

To configure a Message Digest 5 (MD5) password for Label Distribution Protocol (LDP) sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **mpls ldp password option** command in global configuration mode. To disable an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password option** *number* **for** *acl* {**key-chain** *keychain-name* | [**0** | **7**] *password*}

no mpls ldp [**vrf** *vrf-name*] **password option** *number*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding instance (VRF) configured on the label switch router (LSR).
number	The option number. A comparison of the *number* argument from several commands by the software sets up the order in which LDP evaluates access lists in the definition of a password for the neighbor. The valid range is 1 to 32767.
for *acl*	Specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access lists can be used for the *acl* argument.
key-chain *keychain-name*	Specifies the name of the key chain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic.
0 | **7**	(Optional) Specifies whether the *password* that follows is encrypted: • **0** specifies an unencrypted password. • **7** specifies an encrypted password.
password	Specifies the MD5 password to be used for the specified LDP sessions.

Defaults

The MD5 password for LDP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.0(32)SRB.
12.0(33)S	The **key-chain** *keychian-name* keyword-argument pair was added.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies the *password* argument as the MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by an access list specified in the *acl* argument. This password is used if a password is not specified by the **mpls ldp neighbor password** command.

When a configuration includes multiple **mpls ldp password option** commands, the *number* argument defines the order in which the command access lists are evaluated.

A configuration for a VRF can include zero, one, or more **mpls ldp password option** commands.

You can specify the passwords as unencrypted text or encrypted format (type 7). If you configure a type 7 password, the password is saved in encrypted form. If you configure a type 0 password, it can be saved in unencrypted form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, the type 0 password is converted and saved in encrypted form.

  When you enter a **show running-config** command, if the global **service password-encryption** command is enabled, a password saved in unencrypted form is converted into encrypted form, and displayed and saved in encrypted form.
- If the **service password-encryption** command is disabled, the type 0 password is saved in unnencrypted form.

Examples

The following example shows how to configure an MD5 password for an LDP session with neighbors whose LDP router IDs are permitted by access list 10:

```
Router> enable
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls ldp password option 6 for 10 password1
Router(config)# exit
Router#
```

The password, called *password1*in the above example, is unencrypted.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password required

To specify that Label Distribution Protocol (LDP) must use a password for an attempt to establish a session between LDP peers, use the **mpls ldp password required** command in global configuration mode. To remove the requirement that a password be used for a session with LDP, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password required** [**for** *acl*]

no mpls ldp [**vrf** *vrf-name*] **password required** [**for** *acl*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
for *acl*	(Optional) Access list name or number that specifies a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the *acl* argument.

Defaults

If the **vrf** keyword is not specified in the command, the command applies to the global routing table.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command specifies that LDP must always use a password for an attempt to establish a session. If LDP cannot determine the password to use for an LDP session with a neighbor, an LDP session is not established.

The **vrf** keyword is available when you have configured a VRF on the LSR. If you specify a *vrf-name* argument and a VRF with that name is not configured on the LSR, a warning message is displayed and the command is discarded. If you remove a VRF, you also delete the password configured for that VRF.

Each VRF or global routing table can have zero or one **mpls ldp password required** command.

Examples

The following example shows how to specify that LDP must use a password for an attempt to establish a session between LDP peers:

```
Router> enable
Router# configure terminal
```

```
Router(config)# mpls ldp password required
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password rollover duration

To configure the duration before the new password takes effect on an MPLS label switch router (LSR), use the **mpls ldp password rollover duration** command in global configuration mode. To disable duration of a password rollover, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password rollover duration** *minutes*

no mpls ldp [**vrf** *vrf-name*] **password rollover duration** *minutes*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing/forwarding instance (VRF) configured on the label switch router (LSR).
minutes	Specifies the time, in minutes, before password rollover occurs on this router. The range is from 5 to 65535.

Defaults

The MD5 password for LDP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated in Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated in Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

A lossless password rollover takes effect after the configured duration when passwords are configured without the use of a key chain.

Examples

The following example shows how to configure the duration before the new password takes effect on an LSR so there is enough time to successfully change all the passwords on all of the routers. In this example, a duration of 10 minutes is configured before the rollover occurs.

```
mpls ldp password rollover duration 10
```

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.

Command	Description
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
service password-encryption	Encrypts passwords.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp path-vector maxlength

To set the maximum number of router IDs permitted in a path vector type, length, value (TLV) used to perform path vector loop detection, use the **mpls ldp path-vector maxlength** command in global configuration mode. To return the path vector maximum length to the default behavior, use the **no** form of this command.

mpls ldp path-vector maxlength *number*

no mpls ldp path-vector maxlength

Syntax Description

number	Number from 0 to 254, inclusive, that defines the maximum number of 4-octet router IDs permitted in the path vector. The default behavior configured with the **no** form of this command is to track and use the value set by the **mpls ldp maxhops** command (1 to 255). A value of 0 disables the path-vector loop detection feature.

Command Default

If you do not configure this command, the default path vector maximum length value is whatever value is configured for the **mpls ldp maxhops** command. If you reconfigure the maximum hops value, the path vector maximum length value automatically changes to the new maximum hops value. If the **mpls ldp maxhops** command is not configured, the default value is 254.

Command Modes

Global configuration

Command History

Release	Modification
12.3(19)	This command was introduced.
12.4(8)	This command was integrated into Cisco IOS Release 12.4(8).
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

When an ATM label switch router (LSR) initiates a request for a label binding, and path vector loop detection is enabled, the request includes a path vector TLV that contains the router ID of the requesting router. Subsequent ATM LSRs along the path to the edge of the ATM label switching region add their router IDs to the path vector before forwarding the Label Request message to the next hop.

When an ATM LSR receives a Label Request message, it does not send a Label Mapping message in response, nor does it propagate the request to the destination next hop if a loop is detected by the path vector feature. Instead, the ATM LSR returns an error message that specifies that a loop has been detected. A loop is detected if either of the following occurs:

- The path vector length in the request equals or exceeds the configured Path Vector Limit value configured by the **mpls ldp path-vector maxlength** command.
- The receiving ATM LSR finds its own router ID within the path vector list.

Like the maximum hop count, the path vector limit threshold is used to prevent forwarding loops in the setting up of label switch path (LSPs) across an ATM region.

If you configured the **mpls ldp loop-detection** command for ATM LSRs that are sending and receiving Label Request and Label Map messages, you might want to inhibit the use of the path vector for loop detection (**mpls ldp path-vector maxlength 0** command).

To return the maximum path vector length to its default value, which is whatever value is configured for the **mpls ldp maxhops** command, use the **no** form of the **mpls lsp path-vector maxlength** command.

Examples

The following example shows how to set the maximum path vector length to 100 router IDs:

```
configure terminal

mpls ldp path-vector maxlength 100
exit
```

The following example shows the maximum path vector length set to 254, which is verified by you looking at the output from the **show mpls ldp parameters** command or the **show mpls ldp neighbors detail** command:

```
configure terminal

mpls ldp path-vector maxlength 254
exit

Router# show mpls ldp parameters

Protocol version: 1
Downstream label generic region: min label: 16; max label: 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 4
Downstream on Demand Path Vector Limit: 254   !Verifies maximum path-vector length is 254.
!
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: on
Router#

Router# show mpls ldp neighbor detail

Peer LDP Ident: 10.0.3.33:1; Local LDP Ident 10.0.2.93:1
    TCP connection: 10.0.3.33.53366 - 10.0.2.93.646
    State: Oper; Msgs sent/rcvd: 132/123; Downstream on demand
    Up time: 00:24:27; UID: 5; Peer Id 0;
    LDP discovery sources:
      Switch1.1; Src IP addr: 10.0.3.33
        holdtime: 15000 ms, hello interval: 5000 ms
    Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Clients: TC ATM
    Path Vector Loop Detection Peer/Local: On/On
    Path Vector Limit Peer/Local: 4/254  ! Verifies the maximum path-vector length is 254.
Router#
```

Related Commands

Command	Description
mpls ldp loop-detection	Enables the LDP optional loop detection mechanism.
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution.
mpls ldp router-id	Specifies a preferred interface for determining the LDP router ID.
show mpls ldp neighbors	Displays the status of LDP sessions.
show mpls ldp parameters	Displays current LDP parameters.

mpls ldp router-id

To specify a preferred interface for the Label Distribution Protocol (LDP) router ID, use the **mpls ldp router-id** command in global configuration mode. To disable the interface from being used as the LDP router ID, use the **no** form of this command.

mpls ldp router-id [**vrf** *vrf-name*] *interface* [**force**]

no mpls ldp router-id [**vrf** *vrf-name*] [*interface* [**force**]]

Cisco CMTS Routers

mpls ldp router-id gigabitethernet *slot*/*subslot*/*port* [**force**]

no mpls ldp router-id gigabitethernet *slot*/*subslot*/*port* [**force**]

Syntax Description

vrf *vrf-name*	(Optional) Selects the interface as the LDP router ID for the named Virtual Private Network (VPN) routing and forwarding (VRF) table. The selected interface must be associated with the named VRF.
interface	The specified interface to be used as the LDP router ID, provided that the interface is operational.
gigabitethernet *slot*/*subslot*/*port*	Specifies the location of the Gigabit Ethernet interface.
force	(Optional) Alters the behavior of the **mpls ldp router-id** command, as described in the "Usage Guidelines" section.

Command Default

If the **mpls ldp router-id** command is not executed, the router determines the LDP router ID as follows:

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.

Command Modes

Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	The **force** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.4(5)	The **vrf** *vrf-name* keyword/argument pair was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

The **mpls ldp router-id** command allows you to use 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.
3. 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.

The following behaviors apply to the default VRF as well as to VRFs that you explicitly configure with the **vrf** *vrf-name* keyword/argument pair:

- The interface you select as the router ID of the VRF must be associated with the VRF.
- If the interface is no longer associated with the VRF, the **mpls ldp router-id** command that uses the interface is removed.
- If the selected interface is deleted, the **mpls ldp router-id** command that uses the interface is removed.

- If you delete a VRF that you configured, the **mpls ldp router-id** command for the deleted VRF is removed. The default VRF cannot be deleted.

Examples

The following example shows that the POS2/0/0 interface has been specified as the preferred interface for the LDP router ID. The IP address of that interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id pos2/0/0
```

The following example shows that the Ethernet 1/0 interface, which is associated with the VRF vpn-1, is the preferred interface. The IP address of the interface is used as the LDP router ID.

```
Router(config)# mpls ldp router-id vrf vpn-1 eth1/0
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

mpls ldp session protection

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) autoconfiguration for existing LDP sessions or when new sessions are established, use the **mpls ldp session protection** command in **global** configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp session protection [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}]

no mpls ldp session protection [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}]

Syntax Description

vrf *vpn-name*	(Optional) Specifies a VPN routing and forwarding instance (*vpn-name*) for accepting labels. This keyword is available when the router has at least one VRF configured.
for *acl*	(Optional) Specifies a standard IP access control list that contains the prefixes that are to be protected.
duration	(Optional) Specifies the time that the LDP Targeted Hello Adjacency should be retained after a link is lost. **Note** If you use this keyword, you must select either the **infinite** keyword or the *seconds* argument.
infinite	Specifies that the LDP Targeted Hello Adjacency should be retained forever after a link is lost.
seconds	Specifies the time in seconds that the LDP Targeted Hello Adjacency should be retained after a link is lost. The valid range of values is 30 to 2,147,483 seconds.

Defaults

LDP sessions are not established.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is not supported under the following circumstances:

- With TDP sessions
- With extended access lists
- With LC-ATM routers

If you issue the **mpls ldp session protection** command without the **duration** keyword, then session protection is enabled for 86400 seconds (24 hours) meaning that the LDP Targeted Hello Adjacency is retained for 24 hours after a link is lost. This is the default timeout.

If you issue the **mpls ldp session protection duration infinite** command, then session protection is enabled forever meaning that the LDP Targeted Hello Adjacency is retained forever after a link is lost.

If you issue the **mpls ldp session protection duration** *seconds* command, then session protection is enabled for the number of seconds indicated meaning that the LDP Targeted Hello Adjacency is retained for that amount of time. For example, if you issued **mpls ldp session protection duration 100**, then the LDP Targeted Hello Adjacency is retained for 100 seconds after a link is lost.

Examples

In the following example, MPLS LDP Autoconfiguration is enabled for LDP sessions for peers whose router IDs are listed in access control list rtr4:

```
Router(config)# mpls ldp session protection for rtr4
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
show mpls ldp neighbor	Displays the contents of the LDP.

mpls ldp sync

To enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization on interfaces for an Open Shortest Path First (OSPF) process or an Intermediate System-to-Intermediate System (IS-IS) process, use the **mpls ldp sync** command in router configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp sync

no mpls ldp sync

Syntax Description

This command has no arguments or keywords.

Command Default

MPLS LDP-IGP synchronization is not enabled on interfaces belonging to the OSPF or IS-IS processes.

Command Modes

Router configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.0(32)SY	This command is supported on interfaces running IS-IS processes in Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If the **mpls ldp sync** command is configured, you cannot enter the global **no mpls ip** command. If you want to disable LDP synchronization, you must enter the **no mpls ldp igp sync** command first.

The **mpls ldp sync** command is supported with OSPF or IS-IS. Other IGPs are not supported.

Examples

In the following example, MPLS LDP-IGP synchronization is enabled for an OSPF process or an IS-IS process:

```
Router(config-router)# mpls ldp sync
```

Related Commands

Command	Description
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.
no mpls ip	Disables hop-by-hop forwarding.

Command	Description
show isis mpls ldp	Displays synchronization and autoconfiguration information about interfaces belonging to IS-IS processes.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

mpls ldp tcp pak-priority

To give high priority to Label Distribution Protocol (LDP) messages sent by a router locally using Transmission Control Protocol (TCP) connections, use the **mpls ldp tcp pak-priority** command in global configuration mode. To keep LDP messages at normal priority, use the **no** form of this command.

mpls ldp tcp pak-priority

no mpls ldp tcp pak-priority

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

This command allows you to set high priority for LDP messages sent by a router locally using TCP connections.

During heavy network traffic, LDP session keepalive messages can be dropped from the outgoing interface output queue. As a result, keepalives can timeout causing LDP sessions to go down.

First, to avoid session loss due to keepalive timeouts, configure the quality of service (QoS) and differentiated services code point (DSCP) for packets with type of service (ToS) bits set to 6. This configuration guarantees that packets with a ToS bit precedence value of 6 receive a specified percentage of the bandwidth of the designated outgoing links. Second, if you still experience a problem, use the **mpls ldp tcp pak-priority** command.

Note Previously established LDP sessions are not affected when you issue the **mpls ldp tcp pak-priority** or the **no mpls ldp tcp pak-priority** command.

Examples

The following example gives LDP session messages sent by a router high priority locally:

```
Router(config)# mpls ldp tcp pak-priority
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
debug mpls ldp transport connections	Displays information about the TCP connections used to support LDP sessions.

Command	Description
match ip precedence	Identifies IP precedence values as match criteria.
match mpls experimental	Configures a class map to use the specified value of the EXP field as a match criterion.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

mpls load-balance per-label

To enable the load balancing for the tag-to-tag traffic, use the **mpls load-balance per-label** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mpls load-balance per-label

no mpls load-balance per-label

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enable load balancing for the tag-to-tag traffic, the traffic is balanced based on the incoming label (per prefix) among Multiprotocol Label Switching (MPLS) interfaces. Each MPLS interface supports an equal number of incoming labels.

You can use the **show mpls ttfib** command to display the incoming label (indicated by an asterisk) that is included in the load balancer.

Examples

This example shows how to enable the load balancing for the tag-to-tag traffic:

```
Router(config)# mpls load-balance per-label
Router(config)#
```

This example shows how to disable the load balancing for the tag-to-tag traffic:

```
Router(config)# no mpls load-balance per-label
Router(config)#
```

Related Commands

Command	Description
show mpls ttfib	Displays information about the MPLS TTFIB table.

mpls mtu

To set the per-interface Multiprotocol Label Switching (MPLS) maximum transmission unit (MTU) for labeled packets, use the **mpls mtu** command in interface configuration mode. To restore the default, use the **no** form of this command.

mpls mtu [**override**] *bytes*

no mpls mtu

Syntax Description

override	(Optional) Allows you to set the MPLS MTU value higher than the interface MTU value on interfaces (such as Ethernet) that have a default interface MTU value of 1580 or less. The **override** keyword is not available for interface types that do not have a default MTU value of 1580 or less.
bytes	The MTU in bytes includes the label stack in the value.

Command Default

The default MPLS MTU is the MTU configured for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was modified to incorporate new MPLS terminology.
12.2(25)S	The command changed the maximum allowable MPLS MTU values. See the "Usage Guidelines for Cisco IOS Release 12.2(25)S" section for more information.
12.2(27)SBC	The command changed so that you cannot set the MPLS MTU value larger than the interface MTU value. The **override** keyword was introduced. See the "Usage Guidelines for Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and Later Releases" section for more information.
12.(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

Usage Guidelines for Cisco IOS Release 12.2(25)S

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 conditions. A best practice is to set the interface MTU of the core-facing interface to a value greater than either the IP MTU or interface MTU of the edge-facing interface.

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).

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 from 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 system does not accept the MPLS MTU setting. If this happens, reconfigure the MPLS MTU setting to conform to the guidelines.

Usage Guidelines for Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and Later Releases

In 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 value larger than the interface MTU value. This is to prevent conditions such as dropped packets, data corruption, and high CPU rates.

- If you attempt to set the MPLS MTU value higher than the interface MTU value, the software displays the following error, which reminds you to set the interface MTU to a higher value before you set the MPLS MTU value:

  ```
  % Please increase interface mtu to xxxx and then set mpls mtu
  ```

- If you have an interface with a default interface MTU value of 1580 or less (such as an Ethernet interface), the **mpls mtu** command provides the **override** keyword, which allows you to set the MPLS MTU value higher than the interface MTU value. The **override** keyword is not available for interface types that do not have a default interface MTU value of 1580 or less.

Note The **override** keyword is supported in 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases.

- If you have configuration files with MPLS MTU values that are larger than the interface MTU values and you upgrade to Cisco IOS Release 2.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, or a later release, the software does not change the MPLS MTU value. When you reboot the router, the software accepts whatever values are set for the MPLS MTU and the interface MTU. The following error message is displayed during system initialization:

  ```
  Setting the mpls mtu to xxxx on interface x/x, which is higher than the interface MTU
  xxxx. This could lead to packet forwarding problems including packet drops.
  ```

  Set the MPLS MTU values lower than the interface MTU values.

Caution If you do not set the MPLS MTU less than or equal to the interface MTU, data corruption, dropped packets, and high CPU conditions can occur.

- Changing the interface MTU can also modify the IP MTU, Connectionless Network Service (CLNS) MTU, and other MTU values, if they depend on the value of the interface MTU. The Open Shortest Path First (OSPF) routing protocol requires that the IP MTU values match on both ends of the link. Similarly, the Intermediate System-to-Intermediate System (IS-IS) routing protocol requires that the CLNS MTU values match on both ends of the link. If the values on both ends of the link do not match, IS-IS or OSPF cannot complete its initialization.

General Usage Guidelines

- ATM interfaces cannot accommodate packets that exceed the Segmentation and Reassembly (SAR) buffer size, because labels are added to the packet. The *bytes* argument refers to the number of bytes in the packet before the addition of any labels. If each label is 4 bytes, the maximum value of bytes on an ATM interface is the physical MTU minus 4**x* bytes, where *x* is the number of labels expected in the received packet.
- If a labeled IPv4 packet exceeds the MPLS MTU size for the interface, Cisco IOS software fragments the packet. If a labeled non-IPv4 packet exceeds the MPLS MTU size, the packet is dropped.
- All devices on a physical medium must have the same MPLS MTU value in order for MPLS to interoperate.
- The MTU for labeled packets for an interface is determined as follows:
  - If the **mpls mtu** *bytes* command has been used to configure an MPLS MTU, the MTU for labeled packets is the *bytes* value.
  - Otherwise, the MTU for labeled packets is the default MTU for the interface.
- Because labeling a packet makes it larger due to the label stack, you may want the MPLS MTU to be larger than the interface MTU or IP MTU in order to prevent the fragmentation of labeled packets, which would not be fragmented if they were unlabeled. In Cisco IOS Release 12.2(25)S and later releases, the MPLS MTU cannot be larger than the interface MTU.
- Changing the interface MTU value (using the **mtu** interface configuration command) can affect the MPLS MTU of the interface. If the MPLS MTU value is the same as the interface MTU value (this is the default), and you change the interface MTU value, the MPLS MTU value will automatically be set to this new MTU as well. However, the reverse is not true; changing the MPLS MTU value has no effect on the interface MTU.

Examples

The following example shows how to set the interface MTU value and MPLS MTU value for a serial interface:

```
interface Serial4/0
 mtu 1520
 ip unnumbered Loopback0
 mpls mtu 1510
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 ip rsvp bandwidth 2000 2000
```

The following example shows how to set the maximum labeled packet size for the FastEthernet interface to 1508, which is common in an MPLS core carrying MPLS Virtual Private Network (VPN) traffic:

```
interface Fastethernet0
  mpls mtu override 1508
```

Related Commands

Command	Description
mtu	Sets the MTU size for the interface.

mpls netflow egress

To enable Multiprotocol Label Switching (MPLS) egress NetFlow accounting on an interface, use the **mpls netflow egress** command in interface configuration mode. To disable MPLS egress NetFlow accounting, use the **no** form of this command.

mpls netflow egress

no mpls netflow egress

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

Use this command to configure the provider edge (PE) to customer edge (CE) interface of a PE router.

Examples

The following example shows how to enable MPLS egress NetFlow accounting on the egress PE interface that connects to the CE interface at the destination Virtual Private Network (VPN) site:

```
Router(config-if)# mpls netflow egress
```

Related Commands

Command	Description
debug mpls netflow	Enables debugging of MPLS egress NetFlow accounting.
show mpls forwarding-table	Displays a message that the quick flag is set for all prefixes learned from the MPLS egress NetFlow accounting enabled interface.
show mpls interfaces	Displays the value of the output_feature_state.

mpls oam

To enter MPLS OAM configuration mode for customizing the default behavior of echo packets, use the **mpls oam** command in global configuration mode. To disable MPLS OAM functionality, use the **no** format of this command.

mpls oam

no mpls oam

Syntax Description

This command has no arguments or keywords.

Command Default

Customizing the default behavior of echo packets is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	The **no** and **default** keywords were removed.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

After you enter the **mpls oam** command, you can enter the **echo** command in MPLS OAM configuration mode to specify the revision number of the echo packet's default values or to send the vendor's extension type, length, values (TLVs) with the echo packet.

Examples

The following example enters MPLS OAM configuration mode for customizing the default behavior of echo packets:

```
mpls oam
```

Related Commands

Command	Description
echo	Customizes the default behavior of echo packets.
ping mpls	Checks MPLS LSP connectivity.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

mpls prefix-map

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls prefix-map** command is not available in Cisco IOS software.

To configure a router to use a specified quality of service (QoS) map when a label destination prefix matches the specified access list, use the **mpls prefix-map** command in ATM subinterface submode.

mpls prefix-map *prefix-map* **access-list** *access-list* **cos-map** *cos-map*

Syntax Description

prefix-map	Unique number for a prefix map.
access-list *access list*	Unique number for a simple IP access list.
cos-map *cos-map*	Unique number for a QoS map.

Defaults

No access list is linked to a QoS map.

Command Modes

ATM subinterface submode (config-subif)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.4(20)T	This command was removed.

Usage Guidelines

This **mpls prefix-map** command links an access list to a QoS map when a label distribution prefix matches the specified access list.

Examples

The following example shows how to link an access list to a QoS map:

```
Router(config-subif)# mpls prefix-map 55 access-list 55 cos-map 55
```

Related Commands

Command	Description
show mpls prefix-map	Displays the prefix map used to assign a QoS map to network prefixes that match a standard IP access list.

mpls request-labels for

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls request-labels for** command is not available in Cisco IOS software.

To restrict the creation of label switched paths (LSPs) through the use of access lists on the label switch controller (LSC) or label edge router (LER), use the **mpls request-labels for** command in global configuration mode. To restrict the creation of LSPs through the use of access lists on the LSC or LER, use the **no** form of this command.

mpls request-labels for *access-list*

no mpls request-labels for

Syntax Description

access-list	A named or numbered standard IP access list.

Defaults

No LSPs are created using access lists on the LCS or LER.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology.
12.4(20)T	This command was removed.

Usage Guidelines

The command includes the following usage guidelines:

- You can specify either an access list number or name.
- When you create an access list, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.
- If you omit the mask from an IP host address access list specification, 0.0.0.0 is assumed to be the mask.

Examples

The following example shows how to prevent headend label switched controlled virtual circuits (LVCs) from being established from the LSC to all 192.168.x.x destinations. The following commands are added to the LSC configuration:

```
Router(config)# mpls request-labels for 1
Router(config)# access-list 1 deny 192.168.0.0 0.255.255.255
Router(config)# access-list 1 permit any
```

Related Commands

Command	Description
access list	Creates access lists.
ip access-list	Permits or denies access to IP addresses.

mpls static binding ipv4

To bind a prefix to a local or remote label, use the **mpls static binding ipv4** command in global configuration mode. To remove the binding between the prefix and label, use the **no** form of this command.

mpls static binding ipv4 *prefix mask* {*label* | **input** *label* | **output** *nexthop* {**explicit-null** | **implicit-null** | *label*}}

no mpls static binding ipv4 *prefix mask* {*label* | **input** *label* | **output** *nexthop* {**explicit-null** | **implicit-null** | *label*}}

Syntax Description

prefix mask	Specifies the prefix and mask to bind to a label. (When you do not use the **input** or **output** keyword, the specified label is an incoming label.) **Note** Without the arguments, the **no** form of the command removes all static bindings.
label	Binds a prefix or a mask to a local (incoming) label. (When you do not use the **input** or **output** keyword, the specified label is an incoming label.)
input *label*	Binds the specified label to the prefix and mask as a local (incoming) label.
output *nexthop* **explicit-null**	Binds the Internet Engineering Task Force (IETF) Multiprotocol Label Switching (MPLS) IPv4 explicit null label (0) as a remote (outgoing) label.
output *nexthop* **implicit-null**	Binds the IETF MPLS implicit null label (3) as a remote (outgoing) label.
output *nexthop label*	Binds the specified label to the prefix/mask as a remote (outgoing) label.

Command Default

Prefixes are not bound to local or remote labels.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The command output changed.

Usage Guidelines

The **mpls static binding ipv4** command pushes bindings into Label Distribution Protocol (LDP). LDP then needs to match the binding with a route in the Routing Information Base (RIB) or Forwarding Information Base (FIB) before installing forwarding information.

The **mpls static binding ipv4** command installs the specified bindings into the LDP Label Information Base (LIB). LDP will install the binding labels for forwarding use if or when the binding prefix or mask matches a known route.

Static label bindings are not supported for local prefixes, which are connected networks, summarized routes, default routes, and supernets. These prefixes use implicit-null or explicit-null as the local label.

If you do not specify the **input** or **output** keyword, input (local label) is assumed.

For the **no** form of the command:

- If you specify the command name without any keywords or arguments, all static bindings are removed.
- Specifying the prefix and mask but no label parameters removes all static bindings for that prefix or mask.

Examples

In the following example, the **mpls static binding ipv4** command configures a static prefix and label binding before the label range is reconfigured to define a range for static assignment. The output of the command indicates that the binding has been accepted, but cannot be used for MPLS forwarding until you configure a range of labels for static assignment that includes that label.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55

 % Specified label 55 for 10.0.0.0/8 out of configured
 % range for static labels.  Cannot be used for forwarding until
 % range is extended.
Router(config)# end
```

The following **mpls static binding ipv4** commands configure input and output labels for several prefixes:

```
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 2607
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 input 17
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 output 10.13.0.8
explicit-null
Router(config)# end
```

The following **show mpls static binding ipv4** command displays the configured bindings:

```
Router# show mpls static binding ipv4

10.0.0.0/8: Incoming label: 55
  Outgoing labels:
    10.0.0.66   2607
10.66.0.0/24: Incoming label: 17
  Outgoing labels:
    10.13.0.8    explicit-null
```

Related Commands

Command	Description
show mpls forwarding-table	Displays labels currently being used for MPLS forwarding.
show mpls label range	Displays statically configured label bindings.

mpls static binding ipv4 vrf

To bind a prefix to a local label, use the **mpls static binding ipv4 vrf** command in global configuration mode. To remove static binding between the prefix and label, use the **no** form of this command.

mpls static binding ipv4 vrf *vpn-name prefix mask* {**input** *label* | *label*}

no mpls static binding ipv4 vrf *vpn-name prefix mask* [**input** *label* | *label*]

Syntax Description

vpn-name	The VPN routing and forwarding (VRF) instance.
prefix mask	The destination prefix and mask.
input *label*	A local (incoming) label. This argument is optional for the **no** form of the command.
label	A local label. This argument is optional for the **no** form of the command.

Command Default

Label bindings are dynamically assigned.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **mpls static binding ipv4 vrf** command is used only when you configure input labels.

Depending on how you configure the MPLS LDP VRF-Aware Static Labels feature, static labels are advertised one of the following ways:

- By Label Distribution Protocol (LDP) between provider edge (PE) and customer edge (CE) routers within a VRF instance.
- In VPNv4 Border Gateway Protocol (BGP) in the service provider's backbone.

If you do not specify the **input** keyword, an input (local) label is assumed.

The **no** form of the command functions as follows:

- Omitting the prefix and the subsequent parameters removes all static bindings.
- Specifying the prefix and mask but no label parameters removes all static bindings for that prefix or mask.

Examples

The following example binds a prefix to local label 17:

```
Router(config)# mpls static binding ipv4 vrf vpn100 10.66.0.0 255.255.0.0 input 17
```

Related Commands

Command	Description
show mpls static binding ipv4 vrf	Displays configured static bindings.

mpls static crossconnect

To configure a Label Forwarding Information Base (LFIB) entry for the specified incoming label and outgoing interface, use the **mpls static crossconnect** command in global configuration mode. To remove the LFIB entry, use the **no** form of this command.

mpls static crossconnect *inlabel out-interface nexthop* {*outlabel* | **explicit-null** | **implicit-null**}

no mpls static crossconnect *inlabel out-interface nexthop* {*outlabel* | **explicit-null** | **implicit-null**}

Syntax Description

inlabel	The incoming label.
out-interface	The outgoing interface.
nexthop	The destination next-hop router. (Use for multiaccess interfaces only.)
outlabel	The outgoing label.
explicit-null	The IETF MPLS IPv4 explicit null label (0).
implicit-null	The IETF MPLS implicit null label (3).

Command Default

Cross connects are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

You must specify the *nexthop* address for multiaccess interfaces.

Examples

In the following example, the **mpls static crossconnect** command configures a cross connect from incoming label 45 to outgoing label 46 through POS interface POS5/0:

```
Router(config)# mpls static crossconnect 45 pos5/0 46
```

Related Commands

Command	Description
show mpls static crossconnect	Displays statically configured LFIB entries.

mpls traffic-eng

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it floods Multiprotocol Label Switching (MPLS) traffic engineering (TE) link information into the indicated IS-IS level, use the **mpls traffic-eng** command in router configuration mode. To disable the flooding of MPLS TE link information into the indicated IS-IS level, use the **no** form of this command.

mpls traffic-eng {**level-1** | **level-2**}

no mpls traffic-eng {**level-1** | **level-2**}

Syntax Description

level-1	Floods MPLS TE link information into IS-IS level 1.
level-2	Floods MPLS TE link information into IS-IS level 2.

Command Default

Flooding is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

This command, which is part of the routing protocol tree, causes link resource information (such as available bandwidth) for appropriately configured links to be flooded in the IS-IS link-state database.

Examples

The following example shows how to configure MPLS TE link information flooding for IS-IS level 1:

```
Router(config-router)# mpls traffic-eng level-1
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.

mpls traffic-eng administrative-weight

To override the Interior Gateway Protocol (IGP) administrative weight (cost) of the link, use the **mpls traffic-eng administrative-weight** command in interface configuration mode. To disable the override, use the **no** form of this command.

mpls traffic-eng administrative-weight *weight*

no mpls traffic-eng administrative-weight

Syntax Description

weight	Cost of the link.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Examples

The following example shows how to override the IGP cost of the link and set the cost to 20:

```
Router(config-if)# mpls traffic-eng administrative-weight 20
```

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Sets the user-specified attribute flags for an interface.

mpls traffic-eng area

To configure a router running Open Shortest Path First (OSPF) Multiprotocol Label Switching (MPLS) so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** command in router configuration mode. To disable flooding of traffic engineering for the indicated OSPF area, use the **no** form of this command.

mpls traffic-eng area *number*

no mpls traffic-eng area *number*

Syntax Description

number	The OSPF area on which MPLS traffic engineering is enabled.

Defaults

Flooding is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is in the routing protocol configuration tree and is supported for both OSPF and IS-IS. The command affects the operation of MPLS traffic engineering only if MPLS traffic engineering is enabled for that routing protocol instance. Currently, only a single level can be enabled for traffic engineering.

Examples

The following example shows how to configure a router running OSPF MPLS to flood traffic engineering for OSPF 0:

```
Router(config-router)# mpls traffic-eng area 0
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.
router ospf	Configures an OSPF routing process on a router.

mpls traffic-eng atm cos global-pool

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls traffic-eng atm cos global-pool** command is not available in Cisco IOS software.

To specify the class of service for all global pools in traffic engineering tunnels traversing XTagATM interfaces on an ATM-label switch router (LSR), use the **mpls traffic-eng atm cos global-pool** command in global configuration mode.

mpls traffic-eng atm cos global-pool [**available** | **standard** | **premium** | **control**]

Syntax Description

available | **standard** | **premium** | **control**	(Optional) Four classes of service, ordered from lowest priority (**available**) to highest priority (**control**). The default is **available**.

Defaults

The default class is the lowest, **available**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

Because this command works at the global rather than at the interface level, it sets the same class of service for global pool traffic engineering (TE) tunnel traffic on *all* XTagATM interfaces of the device.

Examples

The following example shows how to specify the second-lowest possible priority class of service for the global pool traffic:

```
Router(config)# mpls traffic-eng atm cos global-pool standard
```

Related Commands

Command	Description
mpls traffic-eng atm cos sub-pool	Specifies class of service for subpool traffic traversing XtagATM interfaces.

mpls traffic-eng atm cos sub-pool

Note Effective with Cisco IOS Release 12.4(20)T, the **mpls traffic-eng atm cos sub-pool** command is not available in Cisco IOS software.

To specify the class of service for all subpools in traffic engineering tunnels traversing XTagATM interfaces on an ATM-label switch router (LSR), use the **mpls traffic-eng atm cos sub-pool** command in global configuration mode.

mpls traffic-eng atm cos sub-pool [**available | standard | premium | control**]

Syntax Description

available | standard | premium | control	Four classes of service, ordered from lowest priority (**available**) to highest priority (**control**). The default is **control**.

Defaults

The default class is the highest, **control**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

Because this command works at the global rather than at the interface level, it sets the same class of service for subpool traffic engineering (TE) tunnel traffic on *all* XTagATM interfaces of the device.

Examples

The following example shows how to specify the second-highest possible priority class of service for the subpool traffic:

```
Router(config)# mpls traffic-eng atm cos sub-pool premium
```

Related Commands

Command	Description
mpls traffic-eng atm cos global-pool	Specifies class of service for global-pool traffic traversing XTagATM interfaces.

mpls traffic-eng attribute-flags

To set the user-specified attribute flags for the interface, use the **mpls traffic-eng attribute-flags** command in interface configuration mode. To disable the user-specified attribute flags for the interface, use the **no** form of this command.

mpls traffic-eng attribute-flags *attributes*

no mpls traffic-eng attribute-flags

Syntax Description

attributes	Attributes that will be compared to a tunnel's affinity bits during selection of a path. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

This command assigns attributes to a link so that tunnels with matching attributes (represented by their affinity bits) prefer this link to others that do not match. The interface is flooded globally so that it can be used as a tunnel head-end path selection criterion.

Examples

The following example shows how to set the attribute flags to 0x0101:

```
Router(config-if)# mpls traffic-eng attribute-flags 0x0101
```

Related Commands

Command	Description
mpls traffic-eng administrative-weight	Overrides the IGP administrative weight of the link.
tunnel mpls traffic-eng affinity	Configures affinity (the properties that the tunnel requires in its links) for an MPLS traffic engineering tunnel.

mpls traffic-eng auto-bw timers

To enable automatic bandwidth adjustment for a platform and to start output rate sampling for tunnels configured for automatic bandwidth adjustment, use the **mpls traffic-eng auto-bw timers** command in global configuration mode. To disable automatic bandwidth adjustment for the platform, use the **no** form of this command.

mpls traffic-eng auto-bw timers [**frequency** *seconds*]

no mpls traffic-eng auto-bw timers

Syntax Description

frequency *seconds*	(Optional) Interval, in seconds, for sampling the output rate of each tunnel configured for automatic bandwidth. The value must be from 1 through 604800. The recommended value is 300.

Command Default

When the optional **frequency** keyword is not specified, the sampling interval is 300 seconds (5 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **mpls traffic-eng auto-bw timers** command enables automatic bandwidth adjustment on a platform by causing traffic engineering to periodically sample the output rate for each tunnel configured for bandwidth adjustment.

The **no mpls traffic-eng auto-bw timers** command disables automatic bandwidth adjustment for a platform by terminating the output rate sampling and bandwidth adjustment for tunnels configured for adjustment. 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.

Examples

The following example shows how to designate that for each Multiprotocol Label Switching (MPLS) traffic engineering tunnel, the output rate is sampled once every 10 minutes (every 600 seconds):

```
Router(config)# mpls traffic–eng auto–bw timers frequency 600
```

Related Commands

Command	Description
tunnel mpls traffic-eng auto-bw	Enables automatic bandwidth adjustment for a tunnel, specifies the frequency with which tunnel bandwidth can be automatically adjusted, and designates the allowable range of bandwidth adjustments.
tunnel mpls traffic-eng bandwidth	Configures bandwidth required for an MPLS traffic engineering tunnel.

mpls traffic-eng auto-tunnel backup

To automatically build next-hop (NHOP) and next-next hop (NNHOP) backup tunnels, use the **mpls traffic-eng auto-tunnel backup** command in global configuration mode. To delete the NHOP and NNHOP backup tunnels, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup

no mpls traffic-eng auto-tunnel backup

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **no** form of this command deletes both NHOP and NNHOP backup tunnels that were configured using either the **mpls traffic-eng auto-tunnel backup** command or the **mpls traffic-eng auto-tunnel backup nhop-only** command.

Examples

The following example automatically builds NHOP and NNHOP backup tunnels:

```
Router# mpls traffic-eng auto-tunnel backup
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.

Command	Description
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup config

To enable IP processing without an explicit address, use the **mpls traffic-eng auto-tunnel backup config** command in global configuration mode. To disable IP processing without an explicit address, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup config unnumbered-interface *interface*

no mpls traffic-eng auto-tunnel backup config unnumbered-interface *interface*

Syntax Description

unnumbered-interface *interface*	Interface on which IP processing will be enabled without an explicit address. Default: Loopback0.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example enables IP processing on an Ethernet interface without an explicit address:

```
Router# mpls traffic-eng auto-tunnel backup config unnumbered-interface ethernet1/0
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not currently being used.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup nhop-only

To automatically build next-hop (NHOP) backup tunnels, use the **mpls traffic-eng auto-tunnel backup nhop-only** command in global configuration mode. To delete the NHOP backup tunnels, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup nhop-only

no mpls traffic-eng auto-tunnel backup nhop-only

Syntax Description

This command has no arguments or keywords.

Command Default

The dynamically created backup tunnel uses Loopback0.

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command permits the creation of only NHOP backup tunnels; next-next hop (NNHOP) backup tunnels are not created. The **no** form of this command deletes only the NHOP backup tunnels; NNHOP backup tunnels are not deleted.

Examples

The following example enables the creation of only dynamic NHOP backup tunnels:

```
Router# mpls traffic-eng auto-tunnel backup nhop-only
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup srlg exclude

To specify that autocreated backup tunnels should avoid Shared Risk Link Groups (SRLGs) of the protected interface, use the **mpls traffic-eng auto-tunnel backup srlg exclude** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup srlg exclude [**force** | **preferred**]

no mpls traffic-eng auto-tunnel backup srlg exclude [**force** | **preferred**]

Syntax Description

force	(Optional) Forces the backup tunnel to avoid SRLGs of its protected interfaces.
preferred	(Optional) Causes the backup tunnel to *try* to avoid SRLGs of its protected interfaces, but the backup tunnel can be created if SRLGs cannot be avoided.

Command Default

Autocreated backup tunnels are created without regard to SRLGs.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If you enter the command with either the **force** or **preferred** keyword and then reenter the command with the other keyword, only the last command entered is effective.

Examples

In the following example, backup tunnels must avoid SRLGs of the protected interface:

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
```

In the following example, backup tunnels should *try* to avoid SRLGs of the protected interface:

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude preferred
```

Related Commands

Command	Description
mpls traffic-eng srlg	Configures the SRLG membership of a link (interface).

mpls traffic-eng auto-tunnel backup timers

To configure how frequently a timer will scan backup autotunnels and remove tunnels that are not being used, use the **mpls traffic-eng auto-tunnel backup timers** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup timers removal unused [*sec*]

no mpls traffic-eng auto-tunnel backup timers removal unused [*sec*]

Syntax Description

removal unused [*sec*]	Configures how frequently (in seconds) a timer will scan the backup autotunnels and remove tunnels that are not being used. Valid values are 0 to 604,800.

Command Default

The timer scans backup autotunnels and removes tunnels that are not being used every 3600 seconds (60 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example shows that a timer will scan backup autotunnels every 80 seconds and remove tunnels that are not being used:

```
Router# mpls traffic-eng auto-tunnel backup timers removal unused 80
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.
mpls traffic-eng auto-tunnel backup tunnel-num	Configures the range of tunnel interface numbers for backup autotunnels.

mpls traffic-eng auto-tunnel backup tunnel-num

To configure the range of tunnel interface numbers for backup autotunnels, use the **mpls traffic-eng auto-tunnel backup tunnel-num** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel backup tunnel-num [**min** *num*] [**max** *num*]

no mpls traffic-eng auto-tunnel backup tunnel-num [**min** *num*] [**max** *num*]

Syntax Description

min *num*	(Optional) Minimum number of the backup tunnels. Valid values are from 0 to 65535. Default: 65436.
max *num*	(Optional) Maximum number of the backup tunnels. Valid values are from 0 to 65535. Default: 65535.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example configures the range of backup autotunnel numbers to be between 1000 and 1100:

```
Router# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup	Automatically builds NHOP and NNHOP backup tunnels.
mpls traffic-eng auto-tunnel backup config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel backup nhop-only	Enables the creation of only dynamic next-hop backup tunnels.
mpls traffic-eng auto-tunnel backup timers	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used.

mpls traffic-eng auto-tunnel mesh

To enable autotunnel mesh groups globally, use the **mpls traffic-eng auto-tunnel mesh** command in global configuration mode. To disable autotunnel mesh groups globally, use the **no** form of this command.

mpls traffic-eng auto-tunnel mesh

no mpls traffic-eng auto-tunnel mesh

Syntax Description

This command has no arguments or keywords.

Command Default

Autotunnel mesh groups are not enabled globally.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example shows how to enable autotunnel mesh groups globally:

```
Router(config)# mpls traffic-eng auto-tunnel mesh
```

Related Commands

Command	Description
interface auto-template	Creates the template interface.

mpls traffic-eng auto-tunnel mesh tunnel-num

To configure a range of mesh tunnel interface numbers, use the **mpls traffic-eng auto-tunnel mesh tunnel-num** command in global configuration mode. To use the default values, use the **no** form of this command.

mpls traffic-eng auto-tunnel mesh tunnel-num min *num* **max** *num*

no mpls traffic-eng auto-tunnel mesh tunnel-num

Syntax Description

min *num*	Specifies the beginning number of the range of mesh tunnel interface numbers. Valid values are from 1 to 65535. The default value is 64336.
max *num*	Specifies the ending number of the range of mesh tunnel interface numbers. Valid values are from 1 to 65535. The default value is 65335.

Command Default

The **min** default is 64336. The **max** default is 65335.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If you change an access control list (ACL) and tunnels are deleted because they no longer match the ACL, tunnels that are re-created might not be numbered sequentially; that is, the range of tunnel numbers might not be sequential.

Examples

The following example shows how to specify 1000 as the beginning number of the mesh tunnel interface and 2000 as the ending number:

```
Router(config)# mpls traffic-eng auto-tunnel mesh tunnel-num min 1000 max 2000
```

Related Commands

Command	Description
show mpls traffic-eng auto-tunnel mesh	Displays the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers.

mpls traffic-eng auto-tunnel primary config

To enable IP processing without an explicit address, use the **mpls traffic-eng auto-tunnel primary config** command in global configuration mode. To disable this capability, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary config unnumbered *interface*

no mpls traffic-eng auto-tunnel primary config unnumbered *interface*

Syntax Description

unnumbered *interface*	Interface on which IP processing will be enabled without an explicit address.

Command Default

Loopback0

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example enables IP processing on an Ethernet interface:

```
Router# mpls traffic-eng auto-tunnel primary config unnumbered ethernet1/0
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config mpls ip	Enables LDP on primary autotunnels.
mpls traffic-eng auto-tunnel primary onehop	Automatically creates primary tunnels to all next-hops.
mpls traffic-eng auto-tunnel primary timers	Configures how many seconds after a failure primary autotunnels are removed.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary config mpls ip

To enable Label Distribution Protocol (LDP) on primary autotunnels, use the **mpls traffic-eng auto-tunnel primary config mpls ip** command in global configuration mode. To disable LDP on primary autotunnels, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary config mpls ip

no mpls traffic-eng auto-tunnel primary config mpls ip

Syntax Description

This command has no arguments or keywords.

Command Default

LDP is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example enables LDP on primary autotunnels:

```
Router# mpls traffic-eng auto-tunnel primary config mpls ip
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel primary onehop	Automatically creates primary tunnels to all next hops.
mpls traffic-eng auto-tunnel primary timers	Configures how many seconds after a failure primary autotunnels are removed.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary onehop

To automatically create primary tunnels to all next hops, use the **mpls traffic-eng auto-tunnel primary onehop** command in global configuration mode. To disable the automatic creation of primary tunnels to all next hops, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary onehop

no mpls traffic-eng auto-tunnel primary onehop

Syntax Description

This command has no arguments or keywords.

Command Default

The dynamically created one-hop tunnels use Loopback0.

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example automatically creates primary tunnels to all next hops:

```
Router# mpls traffic-eng auto-tunnel primary onehop
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel primary onehop	Enables LDP on primary autotunnels.
mpls traffic-eng auto-tunnel primary timers	Configures how many seconds after a failure primary autotunnels are removed.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary timers

To configure how many seconds after a failure primary autotunnels are removed, use the **mpls traffic-eng auto-tunnel primary timers** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary timers removal rerouted *sec*

no mpls traffic-eng auto-tunnel primary timers removal rerouted *sec*

Syntax Description

removal rerouted *sec*	Number of seconds after a failure that primary autotunnels are removed. Valid values are 30 to 604,800. Default: 0.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example shows that primary autotunnels are removed 100 seconds after a failure:

```
Router# mpls traffic-eng auto-tunnel primary timers removal rerouted 100
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel primary tunnel-num	Enables LDP on primary autotunnels.
mpls traffic-eng auto-tunnel primary onehop	Automatically creates primary tunnels to all next hops.
mpls traffic-eng auto-tunnel primary tunnel-num	Configures the range of tunnel interface numbers for primary autotunnels.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng auto-tunnel primary tunnel-num

To configure the range of tunnel interface numbers for primary autotunnels, use the **mpls traffic-eng auto-tunnel primary tunnel-num** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls traffic-eng auto-tunnel primary tunnel-num [**min** *num*] [**max** *num*]

no mpls traffic-eng auto-tunnel primary tunnel-num [**min** *num*] [**max** *num*]

Syntax Description

min *num*	(Optional) Minimum number of the primary tunnels. Valid values are from 0 to 65535. Default: 65436.
max *num*	(Optional) Maximum number of the primary tunnels. The **max** number is the minimum number plus 99. Valid values are from 0 to 65535.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example shows that the primary tunnel numbers can be between 2000 and 2100:

```
Router# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel primary config	Enables IP processing without an explicit address.
mpls traffic-eng auto-tunnel primary config mpls ip	Enables LDP on primary autotunnels.
mpls traffic-eng auto-tunnel primary onehop	Automatically creates primary tunnels to all next hops.
mpls traffic-eng auto-tunnel primary timers	Configures how many seconds after a failure primary autotunnels are removed.
show ip rsvp fast-reroute	Displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection.

mpls traffic-eng backup-path

To assign one or more backup tunnels to a protected interface, use the **mpls traffic-eng backup-path** command in interface configuration mode.

mpls traffic-eng backup-path tunnel*tunnel-id*

Syntax Description

tunnel*tunnel-id*	Tunnel ID of the backup tunnel that can be used in case of a failure.

Command Default

No backup tunnels are used if this interface goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(16)ST	With Link Protection, this command selected the one-and-only backup tunnel for a given protected interface. If you enter the command twice, the second occurrence overwrites the first occurrence.
12.0(22)S	You can now enter this command multiple times to select multiple backup tunnels for a given protected interface. This can be done for both Link and Node Protection. The command is supported on the Cisco 10000 series ESRs.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Enter this command on the interface to be protected (Link Protection), or on the interface whose downstream node is being protected (Node Protection). You can enter this command multiple times to select multiple backup tunnels for a given protected interface. An unlimited number of backup tunnels can be assigned to protect an interface. The only limitation is memory. By entering this command on a physical interface, LSPs using this interface (sending data *out of* this interface) can use the indicated backup tunnels if there is a link or node failure.

Examples

The following example assigns backup tunnel 34 to interface POS5/0:

```
Router(config)# interface pos5/0
Router(config-if)# mpls traffic-eng backup-path tunnel34
```

Related Commands

Command	Description
tunnel mpls traffic-eng fast-reroute	Enables an MPLS traffic engineering tunnel to use a backup tunnel if there is a link or node failure (provided that a backup tunnel exists).

mpls traffic-eng backup-path tunnel

To configure the physical interface to use a backup tunnel in the event of a detected failure on that interface, use the **mpls traffic-eng backup-path tunnel** command in interface configuration mode.

mpls traffic-eng backup-path tunnel *interface*

Syntax Description

interface	String that identifies the tunnel interface being created and configured.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(8)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Catalyst 6000 series with the SUP720 processor.
12.2(28)SB	This command was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following example specifies the traffic engineering backup tunnel with the identifier 1000:

```
Router(config-if)# mpls traffic-eng backup-path Tunnel 1000
```

Related Commands

Command	Description
show mpls traffic-eng fast-reroute database	Displays information about existing Fast Reroute configurations.
tunnel mpls traffic-eng fast-reroute	Enables an MPLS traffic engineering tunnel to use a backup tunnel in the event of a link failure (assuming a backup tunnel exists).

mpls traffic-eng ds-te bc-model

To enable a Bandwidth Constraints Model to be used by a router in DiffServ-aware Traffic Engineering, use the **mpls traffic-eng ds-te bc-model** global configuration command. (Using the **no** form of this command selects the default model, which is the Russian Dolls Model.)

mpls traffic-eng ds-te bc-model [**rdm** | **mam]**

no mpls traffic-eng ds-te bc-model [**rdm** | **mam]**

Syntax Description

rdm	Russian Dolls Model. (Described in IETF RFC 4127).
mam	Maximum Allocation Model. (Described in IETF RFC 4125).

Defaults

Russian Dolls Model is the default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

1. The Maximum Allocation Model should be selected when the network administrator needs to ensure isolation across all Class Types without having to use pre-emption, and can afford to risk some QoS degradation of Class Types other than the Preimum Class.
2. The Russian Dolls Model should be selected when the network administrator needs to prevent QoS degradation of all Class Types and can impose pre-emption.

Examples

In the following example,the Maximum Allocation Model is being selected:

```
Router(config)# mpls traffic-eng ds-te bc-model mam
```

mpls traffic-eng ds-te mode

To configure a router to enter DiffServ-aware Traffic Engineering modes which incorporate degrees of the IETF Standard, use the **mpls traffic-eng ds-te mode** global configuration command. Use the **no** form of this command to return the router to the pre-IETF-Standard mode.

mpls traffic-eng ds-te mode [**migration** | **ietf]**

no mpls traffic-eng ds-te mode [**migration** | **ietf]**

Syntax Description

migration	A mode by which the router generates IGP and tunnel signalling according to the pre-IETF standard, but adds TE-class mapping and accepts advertisement in both the pre-IETF and the IETF-Standard formats.
ietf	The "Liberal" IETF mode, by which the router generates IGP advertisement and tunnel signalling according to the IETF Standard and responds to TE-class mapping, yet also accepts advertisement in both the pre-IETF-Standard and IETF-Standard formats.

Defaults

Pre-IETF-Standard mode is the default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

1. Place the router into Migration Mode only if it is still in the pre-IETF Standard ("Traditional") mode, and you want to begin upgrading its network to operate the IETF-Standard form of DS-TE.
2. Place the router into Liberal-IETF Mode only if its network is already in the Migration Mode, and you want to complete the upgrade of that network so it will operate the IETF-Standard form of DS-TE.

Examples

In the following example, the router is configured to operate in Migration Mode:

```
Router(config)# mpls traffic-eng ds-te migration
```

mpls traffic-eng fast-reroute backup-prot-preemption

To change the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted, use the **mpls traffic-eng fast-reroute backup-prot-preemption** command in global configuration mode. To use the default algorithm of minimizing the number of label-switched paths (LSPs) that are demoted, use the **no** form of this command.

mpls traffic-eng fast-reroute backup-prot-preemption [**optimize-bw**]

no mpls traffic-eng fast-reroute backup-prot-preemption

Syntax Description

optimize-bw	(Optional) Minimizes the amount of bandwidth wasted.

Command Default

A minimum number of LSPs are preempted.

Command Modes

Global configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **mpls traffic-eng fast-reroute backup-prot-preemption** command allows you to determine the criteria the router will use when selecting the LSPs that will be preempted.

If you enter the command with the **optimize-bw** keyword, the router chooses LSPs that will waste the least amount of bandwidth.

If you do not enter the **mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw** command, the router preempts as few LSPs as possible.

Each router in the network does not have to use the same algorithm; that is, you can specify **optimize-bw** for some routers in the network but not for others.

You can enter the **mpls traffic-eng fast-re-route backup-prot-preemption** command at any time. If you change the algorithm, it does not affect LSPs that already are protected. It only affects the placement of new LSPs signaled after you enter this command. The command can affect LSPs during the next periodic promotion cycle.

Examples

In the following examples, a next-next hop (NNHOP) backup tunnel has the following characteristics:

- Total backup capacity: 240 units
- Used backup bandwidth: 220 units
- Available backup bandwidth: 20 units

The backup tunnel currently is protecting LSP1 through LSP5, which have the following bandwidth, and do not have backup bandwidth protection (that is, the "bandwidth protection desired" bit was not set via the **tunnel mpls traffic-eng fast-reroute** command):

- LSP1: 10 units
- LSP2: 20 units
- LSP3: 30 units
- LSP4: 60 units
- LSP5: 100 units

As shown, LSP1 through LSP5 use 220 units of bandwidth.

LSP6 has backup bandwidth protection and needs 95 units of bandwidth. Twenty units of bandwidth are available, so 75 more units of bandwidth are needed.

In the following example, backup bandwidth protection is enabled and the amount of wasted bandwidth is minimized:

```
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

LSP2 and LS4 are preempted so that the least amount of bandwidth is wasted.

In the following example, backup protection preemption is enabled and the number of preempted LSPs is minimized:

```
Router(config)# no mpls traffic-eng fast-reroute backup-prot-preemption
```

The router selects the LSP whose bandwidth is next-greater than the required bandwidth. Therefore, the router picks LSP5 because it has the next larger amount of bandwidth over 75. One LSP is demoted. and 25 units of bandwidth are wasted.

Related Commands

Command	Description
show ip rsvp fast bw-protect	Displays information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection.

mpls traffic-eng fast-reroute timers

To specify how often the router considers switching a label switched path (LSP) to a new (better) backup tunnel if additional backup bandwidth becomes available, use the **mpls traffic-eng fast-reroute timers** command in global configuration mode. To disable this timer, set the seconds value to zero or use the **no** form of this command.

mpls traffic-eng fast-reroute timers [**promotion** *seconds*]

no mpls traffic-eng fast-reroute timers

Syntax Description

promotion *seconds*	(Optional) Sets the interval, in seconds, between scans to determine if an LSP should use a new, better backup tunnel. Valid values are from 0 to 604800. A value of 0 disables promotions to a better LSP.

Command Default

The timer is running and is set to a frequency of every 300 seconds (5 minutes). If you enter the **no mpls traffic-eng fast-reroute timers** command, the router returns to this default behavior.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

In the following example, LSPs are scanned every 2 minutes (120 seconds). The router uses this information to consider if the LSPs should be promoted to a better backup tunnel:

```
Router(config)# mpls traffic-eng fast-reroute timers promotion 120
```

mpls traffic-eng flooding thresholds

To set a reserved bandwidth thresholds for a link, use the **mpls traffic-eng flooding thresholds** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mpls traffic-eng flooding thresholds {**down** | **up**} *percent* [*percent* ...]

no mpls traffic-eng flooding thresholds {**down** | **up**}

Syntax Description

down	Sets the thresholds for decreased reserved bandwidth.
up	Sets the thresholds for increased reserved bandwidth.
percent [*percent*]	Bandwidth threshold level. For the **down** keyword, valid values are from 0 through 99. For the **up** keyword, valid values are from 1 through 100.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.

Usage Guidelines

When a threshold is crossed, Multiprotocol Label Switching (MPLS) traffic engineering link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding is disabled.

Examples

The following example shows how to set the reserved bandwidth of the link for decreased (down) and for increased (up) thresholds:

```
Router(config-if)# mpls traffic-eng flooding thresholds down 100 75 25
Router(config-if)# mpls traffic-eng flooding thresholds up 25 50 100
```

Related Commands

Command	Description
mpls traffic-eng link timers periodic-flooding	Sets the length of the interval used for periodic flooding.
show mpls traffic-eng link-management advertisements	Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.

mpls traffic-eng interface

To enable Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) link-state advertisement (LSA) for an interface to be advertised into the Open Shortest Path First (OSPF) area 0, use the **mpls traffic-eng interface** command in router configuration mode. To restore the setting of the MPLS TE LSA to the same area as the router LSA, use the **no** form of this command.

mpls traffic-eng interface *interface* **area 0**

no mpls traffic-eng interface *interface* **area 0**

Syntax Description

interface	The interface to be advertised with an MPLS TE LSA into OSPF area 0. The interface may be one or two words.

Defaults

The default is to advertise the area assigned to the interface by the OSPF network configuration.

Command Modes

Router configuration

Command History

Release	Modification
12.0(12)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Usually, the MPLS TE LSA is advertised into the same area as the router LSA. If a link between two Area Border Routers (ABRs) is in an OSPF area besides area 0, you can advertise the link between ABRs into area 0. This solves for TE the same problem that virtual links solve for IP routing. This command is valid only for OSPF. Issue the command on both ABRs for the interfaces at both ends of the link.

Examples

In the following example, OSPF advertises the MPLS TE LSA for interface pos2/0 to area 0:

```
Router(config)# router ospf 1
Router(config-router)# mpls traffic-eng interface pos2/0 area 0
```

Related Commands

Command	Description
mpls traffic-eng multicast-intact	Enables multicast-intact support from the OSPF routing protocol to maintain and publish the native IP nexthops (paths) for every OSPF route.

mpls traffic-eng link timers bandwidth-hold

To set the length of time that bandwidth is held for a Resource Reservation Protocol (RSVP) PATH (Set Up) message while waiting for the corresponding RSVP RESV message to come back, use the **mpls traffic-eng link timers bandwidth-hold** command in global configuration mode.

mpls traffic-eng link timers bandwidth-hold *hold-time*

Syntax Description

hold-time	Sets the length of time that bandwidth can be held. The range is from 1 to 300 seconds.

Defaults

15 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the length of time that bandwidth is held to 10 seconds.

```
Router(config)# mpls traffic-eng link-management timers bandwidth-hold 10
```

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.

mpls traffic-eng link timers periodic-flooding

To set the length of the interval used for periodic flooding, use the **mpls traffic-eng link timers periodic-flooding** command in global configuration mode.

mpls traffic-eng link timers periodic-flooding *interval*

Syntax Description

interval	Length of interval used for periodic flooding (in seconds). The range is from 0 to 3600. If you set this value to 0, you turn off periodic flooding. If you set this value anywhere in the range from 1 to 29, it is treated as 30.

Defaults

180 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set the interval for periodic flooding of traffic engineering (TE) topology information.

Changes in the Multiprotocol Label Switching (MPLS) TE topology database are flooded by the link state Interior Gateway Protocol (IGP). Some changes, such as those to link status (up/down) or configured parameters, trigger immediate flooding. Other changes are considered less urgent and are flooded periodically. For example, changes to the amount of link bandwidth allocated to TE tunnels are flooded periodically unless the change causes the bandwidth to cross a configurable threshold.

Examples

The following example sets the interval length for periodic flooding to advertise flooding changes to 120 seconds.

```
Router(config)# mpls traffic-eng timers periodic-flooding 120
```

Related Commands

Command	Description
mpls traffic-eng flooding thresholds	Sets the reserved bandwidth thresholds of a link.

mpls traffic-eng link-management timers bandwidth-hold

To set the length of time that bandwidth is held for an RSVP path (setup) message while you wait for the corresponding RSVP Resv message to come back, use the **mpls traffic-eng link-management timers bandwidth-hold** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng link-management timers bandwidth-hold *hold-time*

no mpls traffic-eng link-management timers bandwidth-hold

Syntax Description

hold-time	Length of time that bandwidth can be held. Valid values are from 1 to 300 seconds.

Defaults

15 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, bandwidth is set to be held for 10 seconds:

```
Router(config)# mpls traffic-eng link-management timers bandwidth-hold 10
```

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.

mpls traffic-eng link-management timers periodic-flooding

To set the length of the interval for periodic flooding, use the **mpls traffic-eng link-management timers periodic-flooding** command in global configuration mode. To disable the specified interval length for periodic flooding, use the **no** form of this command.

mpls traffic-eng link-management timers periodic-flooding *interval*

no mpls traffic-eng link-management timers periodic-flooding

Syntax Description

interval	Length of the interval (in seconds) for periodic flooding. Valid values are from 0 to 3600. A value of 0 turns off periodic flooding. If you set this value from 1 to 29, it is treated as 30.

Defaults

180 seconds (3 minutes)

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to advertise link state information changes that do not trigger immediate action. For example, a change to the amount of allocated bandwidth that does not cross a threshold.

Examples

The following example shows how to set the interval length for periodic flooding to 120 seconds:

```
Router(config)# mpls traffic-eng link-management timers periodic-flooding 120
```

Related Commands

Command	Description
mpls traffic-eng flooding thresholds	Sets a link's reserved bandwidth thresholds.

mpls traffic-eng logging lsp

To log certain traffic engineering label switched path (LSP) events, use the **mpls traffic-eng logging lsp** command in global configuration mode. To disable logging of LSP events, use the **no** form of this command.

mpls traffic-eng logging lsp {**path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns**} [*acl-number*]

no mpls traffic-eng logging lsp {**path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns**} [*acl-number*]

Syntax Description

path-errors	Logs RSVP path errors for traffic engineering LSPs.
reservation-errors	Logs RSVP reservation errors for traffic engineering LSPs.
preemption	Logs events related to the preemption of traffic engineering LSPs.
setups	Logs events related to the establishment of traffic engineering LSPs.
teardowns	Logs events related to the removal of traffic engineering LSPs.
acl-number	(Optional) Uses the specified access list to filter the events that are logged. Logs events only for LSPs that match the access list.

Defaults

Logging of LSP events is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to log path errors for LSPs that match access list 3:

```
Router(config)# mpls traffic-eng logging lsp path-errors 3
```

Related Commands

Command	Description
access-list (extended)	Defines an extended IP access list.
logging console	Limits the number of messages logged to the console.
mpls traffic-eng logging tunnel	Logs certain traffic engineering tunnel events.
show logging	Displays the messages that are logged in the buffer.

mpls traffic-eng logging tunnel

To log certain traffic engineering tunnel events, use the **mpls traffic-eng logging tunnel** command in global configuration mode. To disable logging of traffic engineering tunnel events, use the **no** form of this command.

mpls traffic-eng logging tunnel lsp-selection [*acl-number*]

no mpls traffic-eng logging tunnel lsp-selection [*acl-number*]

Syntax Description

lsp-selection	Logs events related to the selection of a label switched path (LSP) for a traffic engineering tunnel.
acl-number	(Optional) Uses the specified access list to filter the events that are logged. Logs events only for tunnels that match the access list.

Defaults

Logging of tunnel events is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to log traffic engineering tunnel events associated with access list 3:

```
Router(config)# mpls traffic-eng logging tunnel lsp-selection 3
```

Related Commands

Command	Description
access-list (extended)	Creates an extended access list.
logging console	Limits the number of messages logged to the console.
mpls traffic-eng logging lsp	Logs certain traffic engineering LSP events.
show logging	Displays the messages that are logged in the buffer.

mpls traffic-eng lsp attributes

To create or modify a label switched path (LSP) attribute list, use the **mpls traffic-eng lsp attributes** command in global configuration mode. To remove a specified LSP attribute list from the device configuration, use the **no** form of this command.

mpls traffic-eng lsp attributes *string*

no mpls traffic-eng lsp attributes *string*

Syntax Description

string	LSP attributes list identifier.

Command Default

An LSP attribute list is not created unless you create one.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command sets up an LSP attribute list and enters LSP Attributes configuration mode, in which you can enter LSP attributes.

To associate the LSP attributes and LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

An LSP attribute referenced by the path option takes precedence over the values configured on the tunnel interface. If an attribute is not specified in the LSP attribute list, the devices takes the attribute from the tunnel configuration. LSP attribute lists do not have default values. If the attribute is not configured on the tunnel, then the device uses tunnel default values.

Once you type the **mpls traffic-eng lsp attributes** command, you enter the LSP Attributes configuration mode where you define the attributes for the LSP attribute list that you are creating.

The mode commands are as follows:

- **affinity**—Specifies attribute flags for links that make up an LSP.
- **auto-bw**—Specifies automatic bandwidth configuration.
- **bandwidth**—Specifies LSP bandwidth.
- **lockdown**—Disables reoptimization for the LSP.
- **priority**—Specifies LSP priority.

- **protection**—Enables failure protection.
- **record-route**—Records the route used by the LSP.

The following monitoring and management commands are also available in the LSP Attributes configuration mode:

- **exit**—Exits from LSP Attributes configuration mode.
- **list**—Relists all the entries in the LSP attribute list.
- **no**—Removes a specific attribute from the LSP attribute list.

Examples

The following example shows how to set up an LSP attribute list identified with the numeral 6 with the **bandwidth** and **priority** mode commands. The example also shows how to use the **list** mode command:

```
Router(config)# mpls traffic-eng lsp attributes 6
Router(config-lsp-attr)# bandwidth 500
Router(config-lsp-attr)# list

LIST 6
 bandwidth 500

Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list

LIST 6
 bandwidth 500
 priority 1 1

Router(config-lsp-attr)# exit
```

Related Commands

Command	Description
show mpls traffic-eng lsp attributes	Displays global LSP attributes lists.

mpls traffic-eng mesh-group

To configure a mesh group in an Interior Gateway Protocol (IGP) to allow Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switch routers (LSRs) that belong to the same mesh group to signal tunnels to the local router, use the **mpls traffic-eng mesh-group** command in router configuration mode. To disable signaling of tunnels from LSRs in the same mesh group to the local router, use the **no** form of this command.

mpls traffic-eng mesh-group *mesh-group-id type number* **area** *area-id*

no mpls traffic-eng mesh-group *mesh-group-id type number* **area** *area-id*

Syntax Description

mesh-group-id	Number that identifies a specific mesh group.
type	Type of interface.
number	Interface number.
area *area-id*	Specifies an IGP area.

Command Default

No tunnels are signaled for routers in the same mesh group.

Command Modes

Router configuration (config-router)#

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure a mesh group in an IGP. This allows the MPLS TE LSRs that belong to the specified mesh group to signal tunnels to the local router. The IGP floods mesh group configuration to all routers belonging to the same mesh group. An autotemplate determines how a router participates in an autotunnel. A router can participate in a mesh group through two-way tunnels or one-way tunnels.

Open Shortest Path First (OSPF) is the only IGP supported for the MPLS Traffic Engineering—AutoTunnel Mesh Groups feature.

Examples

The following example shows how to configure OSPF to allow LSRs that belong to the same mesh group (mesh group 10) to signal tunnels to the local router:

```
Router(config)# router ospf 100
Router(config-router)# mpls traffic-eng mesh-group 10 loopback 0 area 100
```

Related Commands

Command	Description
tunnel destination mesh-group	Configures an autotemplate to signal tunnels to all other members of a specified mesh group.

mpls traffic-eng multicast-intact

To configure a router running Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) so that Protocol-Independent Multicast (PIM) and Multiprotocol Label Switching (MPLS) traffic engineering (TE) can work together, use the **mpls traffic-eng multicast-intact** command in router configuration mode. To disable interoperability between PIM and MPLS TE, use the **no** form of this command.

mpls traffic-eng multicast-intact

no mpls traffic-eng multicast-intact

Syntax Description

This command has no arguments or keywords.

Defaults

PIM and MPLS TE do not work together.

Command Modes

Router configuration

Command History

Release	Modification
12.0(12)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **mpls traffic-eng multicast-intact** command allows PIM to use the native hop-by-hop neighbors while unicast routing is using MPLS TE tunnels.

This command works only for OSPF and IS-IS protocols.

Examples

The following example shows how to enable PIM and MPLS TE to interoperate:

```
Router(config)# router ospf 1
Router(config-router)# mpls traffic-eng multicast-intact
```

Related Commands

Command	Description
mpls traffic-eng interface	Configures a router running OSPF or IS-IS so that it floods MPLS TE link information in the indicated OSPF area or IS-IS level.
show ospf routes multicast-intact	Displays multicast-intact paths of OSPF routes.

mpls traffic-eng passive-interface

To configure a link as a passive interface between two Autonomous System Boundary Routers (ASBRs), use the **mpls traffic-eng passive-interface** command in interface configuration mode. To disable the passive link, use the **no** form of this command.

mpls traffic-eng passive-interface nbr-te-id *te-router-id* [**nbr-if-addr** *if-addr*] [**nbr-igp-id** {**isis** *sysid* | **ospf** *sysid*}]

no mpls traffic-eng passive-interface nbr-te-id *te-router-id* [**nbr-if-addr** *if-addr*] [**nbr-igp-id**{**isis** *sysid* | **ospf** *sysid*}]

Syntax Description

nbr-te-id *te-router-id*	Traffic engineering router ID of the neighbor router on the remote side of the link where this command is configured.
nbr-if-addr *if-addr*	(Optional) Interface address of the remote ASBR.
nbr-igp-id	(Optional) Specifies a unique *sysid* for neighboring Interior Gateway Protocols (IGPs) when two or more autonomous systems use different IGPs and have more than one neighbor on the link. Enter the **nbr-igp-id** keyword (followed by the **isis** or **ospf** keyword) and the *sysid* for each IGP. The *sysid* must be unique for each neighbor.
isis *sysid*	System identification of Intermediate System-to-Intermediate System (IS-IS).
ospf *sysid*	System identification of Open Shortest Path First (OSPF).

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	The **nbr-if-addr** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **mpls traffic-eng passive-interface** command sets the next-hop address for a passive interface. The command is required only for a broadcast link.

Enter the **mpls traffic-eng passive-interface** command only on the outgoing interface on which the label-switched path (LSP) will exit; you do not have to enter this command on both ends of the interautonomous system (Inter-AS) link.

On a point-to-point link or on a multiaccess link where there is only one neighbor, you do not have to enter the **isis** or **ospf** keyword (or the *sysid* argument).

If two autonomous systems use different IGPs and have more than one neighbor on the link, you must enter the **nbr-igp-id** keyword followed by **isis** or **ospf** and the *sysid*. The *sysid* must be unique for each neighbor.

For a broadcast link (that is, other Resource Reservation Protocol (RSVP)) features are using the passive link), you must enter the **nbr-if-addr** keyword.

For an RSVP Hello configuration on an Inter-AS link, all keywords are required.

Examples

In the following example there is only one neighbor:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.10.10
```

In the following example, two autonomous systems use different IGPs and have more than one neighbor on the link:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.11.12 nbr-igp-id
ospf 10.10.15.18
```

If autonomous system 1 (AS1) is running IS-IS and AS2 is running OSPF, the unique ID on A1 must be in the system ID format. To form the system ID, we recommend that you append zeros to the router ID of the neighbor. For example, if the AS2 router is 10.20.20.20, then you could enter a system ID of 10.0020.0020.0020.00 for IS-IS on the AS1 router.

In the following example there is a remote ASBR and an IS-IS:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.20.20.20 nbr-igp-id
isis 10.0020.0020.0020.00
```

In the following example, there is a broadcast link and the interface address of the remote ASBR is 10.0.0.2:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.10.10 nbr-if-addr
10.0.0.2
```

mpls traffic-eng path-option list

To configure a path option list, use the **mpls traffic-eng path-option list** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng path-option list [**name** *pathlist-name* | **identifier** *pathlist-number*]

no mpls traffic-eng path-option list [**name** *pathlist-name* | **identifier** *pathlist-number*]

Syntax Description

name *pathlist-name*	Specifies the name of the path option list.
identifier *pathlist-number*	Specifies the identification number of the path option list. Valid values are from 1 through 65535.

Command Default

There are no path option lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

A path option list contains a list of backup paths for a primary path option. You can specify a path option list by entering its name or identifier.

After you enter the **mpls traffic-eng path-option list** command, the router enters path option list configuration mode and you can enter the following commands:

- **path-option**—Specifies the name or identification number of the next path option to add, edit, or delete.
- **list**—Lists all path options.
- **no**—Deletes a specified path option.
- **exit**—Exits from path option list configuration mode.

Then you can specify explicit backup paths by entering their name or identifier.

Examples

The following example configures the path option list named pathlist-01, adds path option 10, lists the backup path that is in the path option list, and exits from path option list configuration mode:

```
Router(config)# mpls traffic-eng path-option list name pathlist-01
Router(cfg-pathoption-list)# path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# list
 path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# exit
```

Related Commands

Command	Description
tunnel mpls traffic-eng path option	Configures a path option for an MPLS TE tunnel.
tunnel mpls traffic-eng path-option protect	Configures a secondary path option or a path option list for an MPLS TE tunnel.

mpls traffic-eng path-selection metric

To specify the metric type to use for path selection for tunnels for which the metric type has not been explicitly configured, use the **mpls traffic-eng path-selection metric** command in global configuration mode. To remove the specified metric type, use the **no** form of this command.

mpls traffic-eng path-selection metric {**igp** | **te**}

no mpls traffic-eng path-selection metric

Syntax Description

igp	Use the Interior Gateway Protocol (IGP) metric.
te	Use the traffic engineering metric.

Defaults

The default is the **te** metric.

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify the metric type to be used for traffic engineering (TE) tunnels for which the **tunnel mpls traffic-eng path-selection metric** command has not been specified.

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the **tunnel mpls traffic-eng path-selection metric** command was entered to specify a metric type for the tunnel, use that metric type.
- Otherwise, if the **mpls traffic-eng path-selection metric** was entered to specify a metric type, use that metric type.
- Otherwise, use the default (**te**) metric.

Examples

The following command specifies that if a metric type was not specified for a given TE tunnel, the igp metric should be used for tunnel path calculation:

```
Router(config)# mpls traffic-eng path-selection metric igp
```

Related Commands

Command	Description
tunnel mpls traffic-eng path-selection metric	Specifies the metric type to use when calculating a tunnel's path.

mpls traffic-eng reoptimize

To force immediate reoptimization of all traffic engineering tunnels, use the **mpls traffic-eng reoptimize** command in privileged EXEC mode.

mpls traffic-eng reoptimize

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to reoptimize all traffic engineering tunnels immediately:

```
Router# mpls traffic-eng reoptimize
```

Related Commands

Command	Description
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.

mpls traffic-eng reoptimize events

To turn on automatic reoptimization of Multiprotocol Label Switching (MPLS) traffic engineering when certain events occur, such as when an interface becomes operational, use the **mpls traffic-eng reoptimize events** command in global configuration mode. To disable automatic reoptimization, use the **no** form of this command.

mpls traffic-eng reoptimize events link-up

no mpls traffic-eng reoptimize events link-up

Syntax Description

link-up	Triggers automatic reoptimization whenever an interface becomes operational.

Defaults

Event-based reoptimization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to turn on automatic reoptimization whenever an interface becomes operational:

```
Router(config)# mpls traffic-eng reoptimize events link-up
```

Related Commands

Command	Description
mpls traffic-eng logging lsp	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng reoptimize	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.

mpls traffic-eng reoptimize timers delay

To delay removal of old label switched paths (LSPs) or installation of new LSPs after tunnel reoptimization, use the **mpls traffic-eng reoptimize timers delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

mpls traffic-eng reoptimize timers delay {**cleanup** *delay-time* | **installation** *delay-time*}

no mpls traffic-eng reoptimize timers delay {**cleanup** *delay-time* | **installation** *delay-time*}

Syntax Description

cleanup *delay-time*	Delays removal of old LSPs after tunnel reoptimization for the specified number of seconds. The valid range is from 0 to 60 seconds. A value of 0 disables the delay. The default is 10 seconds.
installation *delay-time*	Delays installation of new LSPs with new labels after tunnel reoptimization for the specified number of seconds. The valid range is from 0 to 3600 seconds. A value of 0 disables the delay. The default is 3 seconds.

Command Default

Removal of old LSPs and installation of new LSPs is not delayed.

Command Modes

Global configuration

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A device with Multiprotocol Label Switching traffic engineering (MPLS TE) tunnels periodically examines tunnels with established LSPs to discover if more efficient LSPs (paths) are available. If a better LSP is available, the device signals the more efficient LSP; if the signaling is successful, the device replaces the older LSP with the new, more efficient LSP.

Sometimes the slower router-point nodes may not yet utilize the new label's forwarding plane. In this case, if the headend node replaces the labels quickly, it can result in brief packet loss. By delaying the cleanup of the old LSP using the **mpls traffic-eng reoptimize timers delay** cleanup command, packet loss is avoided.

Examples

The following example shows how to set the reoptimization cleanup delay time to one minute:

```
Router# configure
Router(config)# mpls traffic-eng reoptimize timers delay cleanup 60
```

The following example shows how to set the reoptimization installation delay time to one hour:

```
Router# configure
Router(config)# mpls traffic-eng reoptimize timers delay installation 5
```

Related Commands

Command	Description
mpls traffic-eng reoptimize	Forces immediate reoptimization of all traffic engineering tunnels.
mpls traffic-eng reoptimize events	Turns on automatic reoptimization of MPLS traffic engineering when certain events occur, such as when an interface becomes operational.
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.

mpls traffic-eng reoptimize timers frequency

To control the frequency with which tunnels with established label switched paths (LSPs) are checked for better LSPs, use the **mpls traffic-eng reoptimize timers frequency** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng reoptimize timers frequency *seconds*

no mpls traffic-eng reoptimize timers frequency

Syntax Description

seconds	Sets the frequency of reoptimization (in seconds). A value of 0 disables reoptimization. The range of values is 0 to 604800 seconds (1 week).

Defaults

3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP seems to be available, the device attempts to signal the better LSP; if the signaling is successful, the device replaces the old, inferior LSP with the new, better LSP.

Note If the **lockdown** keyword is specified with the **tunnel mpls traffic-eng path-option** command, then a reoptimize check is not done on the tunnel.

If you configure a traffic engineering tunnel with an explicit path that is not fully specified (a series of router IDs or a combination of router IDs and interface addresses), then reoptimization may not occur.

Note If you specify a low reoptimization frequency (for example, less than 30 seconds), there may be an increase in CPU utilization for configurations with a large number of traffic engineering tunnels.

Examples

The following example shows how to set the reoptimization frequency to 1 day:

```
Router(config)# mpls traffic-eng reoptimize timers frequency 86400
```

Related Commands

Command	Description
mpls traffic-eng reoptimize	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.
tunnel mpls traffic-eng path-option	Configures a path option for an MPLS traffic engineering tunnel.

mpls traffic-eng router-id

To specify that the traffic engineering router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** command in router configuration mode. To remove the traffic engineering router identifier, use the **no** form of this command.

mpls traffic-eng router-id *interface-name*

no mpls traffic-eng router-id

Syntax Description

interface-name	Interface whose primary IP address is the router's identifier.

Defaults

No traffic engineering router identifier is specified.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This router identifier acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the traffic engineering router identifier of the destination node, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.

You should configure the same traffic engineering router id for all Interior Gateway Protocol (IGP) routing processes.

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with interface Loopback0:

```
Router(config-router)# mpls traffic-eng router-id Loopback0
```

Related Commands

Command	Description
mpls atm control-vc	Turns on flooding of MPLS traffic engineering link information in the indicated IGP level/area.

mpls traffic-eng scanner

To specify how often Intermediate System-to-Intermediate System (IS-IS) extracts traffic engineering type, length, values (TLVs) objects from flagged label switched paths (LSPs) and passes them to the traffic engineering topology database, and the maximum number of LSPs that the router can process immediately, use the **mpls traffic-eng scanner** command in router configuration mode. To disable the frequency that IS-IS extracts traffic engineering TLVs and the maximum number of LSPs IS-IS passes to the traffic engineering topology database, use the **no** form of this command.

mpls traffic-eng scanner [**interval** *seconds*] [**max-flash** *LSPs*]

no mpls traffic-eng scanner

Syntax Description

interval *seconds*	(Optional) Frequency, in seconds, at which IS-IS sends traffic engineering TLVs into the traffic engineering database. The value can be from 1 to 60. The default value is 5.
max-flash *LSPs*	(Optional) Maximum number of LSPs that the router can process immediately without incurring a delay. The value can be from 0 to 200. The default value is 15.

Command Default

IS-IS sends traffic engineering TLVs into the traffic engineering topology database every 5 seconds after the first 15 LSPs are processed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When IS-IS receives a new LSP, it inserts it into the IS-IS database. If the LSP contains traffic engineering TLVs, IS-IS flags the LSPs for transmission to the traffic engineering database. Depending on the default or user-specified interval, traffic engineering TLVs are extracted and sent to the traffic engineering database. Users can also specify the maximum number of LSPs that the router can process immediately. Processing entails checking for traffic engineering TLVs, extracting them, and passing them to the traffic engineering database. If more than 50 LSPs need to be processed, there is a delay of 5 seconds for subsequent LSPs.

The first 15 LSPs are sent without a delay into the traffic engineering database. If more LSPs are received, the default delay of 5 seconds applies.

If you specify the **no** form of this command, there is a delay of 5 seconds before IS-IS scans its database and passes traffic engineering TLVs associated with flagged LSPs to the traffic engineering database

Examples

In the following example, the router is allowed to process up to 50 IS-IS LSPs without any delay.

```
Router(config)# router isis
Router(config-router)# mpls traffic-eng scanner interval 5 max-flash 50
```

Related Commands

Command	Description
mpls traffic-eng	Configures a router running IS-IS so that it floods MPLS traffic engineering link information into the indicated IS-IS level.
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

mpls traffic-eng signalling advertise implicit-null

To use the Multiprotocol Label Switching (MPLS) encoding for the implicit-null label in signaling messages sent to neighbors that match the specified access list, use the **mpls traffic-eng signalling advertise implicit-null** command in router configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng signalling advertise implicit-null [*acl-name* | *acl-number*]

no mpls traffic-eng signalling advertise implicit-null

Syntax Description

acl-name	Name of the access list.
acl-number	Number of the access list.

Defaults

Use the Cisco encoding for the implicit-null label in signaling messages.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)ST	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure the router to use MPLS encoding for the implicit-null label when it sends signaling messages to certain peers:

```
Router(config-router)# mpls traffic-eng signalling advertise implicit-null
```

mpls traffic-eng srlg

To configure the Shared Risk Link Group (SRLG) membership of a link (interface), use the **mpls traffic-eng srlg** command in interface configuration mode. To remove a link from membership of one or more SRLGs, use the **no** form of this command.

mpls traffic-eng srlg [*num*]

no mpls traffic-eng srlg [*num*]

Syntax Description

num	(Optional) SRLG identifier. Valid values are 0 to 4294967295.

Command Default

A link does not have membership in any SRLG.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can enter the **mpls traffic-eng srlg** command multiple times to make a link a member of multiple SRLGs.

Examples

The following example makes the interface a member of SRLG 5:

```
Router(config-if)# mpls traffic-eng srlg 5
```

If you enter the following commands, the interface is a member of both SRLG 5 and SRLG 6:

```
Router(config-if)# mpls traffic-eng srlg 5
Router(config-if)# mpls traffic-eng srlg 6
```

To remove a link from membership of SRLG 5, enter the following command:

```
Router(config-if)# no mpls traffic-eng srlg 5
```

To remove a link from membership of all SRLGs, enter the following command:

```
Router(config-if)# no mpls traffic-eng srlg
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup srlg exclude	Specifies that autocreated backup tunnels should avoid SRLGs of the protected interface.

mpls traffic-eng topology holddown sigerr

To specify the amount of time that a router ignores a link in its traffic engineering topology database in tunnel path Constrained Shortest Path First (CSPF) computations following a traffic engineering tunnel error on the link, use the **mpls traffic-eng topology holddown sigerr** command in global configuration mode. To disable the time set to ignore a ink following a traffic engineering tunnel error on the link, use the **no** form of this command.

mpls traffic-eng topology holddown sigerr *seconds*

no mpls traffic-eng topology holddown sigerr

Syntax Description

seconds	Length of time (in seconds) a router should ignore a link during tunnel path calculations following a traffic engineering tunnel error on the link. The value can be from 0 to 300.

Command Default

If you do not specify this command, tunnel path calculations ignore a link on which there is a traffic engineering error until either 10 seconds have elapsed or a topology update is received from the Interior Gateway Protocol (IGP).

Command Modes

Global configuration

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

A router that is at the headend for traffic engineering tunnels might receive a Resource Reservation Protocol (RSVP) No Route error message for an existing tunnel or for one being signaled due to the failure of a link the tunnel traffic traverses before the router receives a topology update from the IGP routing protocol announcing that the link is down. In such a case, the headend router ignores the link in subsequent tunnel path calculations to avoid generating paths that include the link and are likely to fail when signaled. The link is ignored until the router receives a topology update from its IGP or a link hold-down timeout occurs. You can use the **mpls traffic-eng topology holddown sigerr** command to change the link hold-down time from its 10-second default value.

Examples

In the following example, the link hold-down time for signaling errors is set at 15 seconds:

```
Router(config)# mpls traffic-eng topology holddown sigerr 15
```

Related Commands

Command	Description
show mpls traffic-eng topology	Displays the MPLS traffic engineering global topology as currently known at the node.

mpls traffic-eng tunnels (global configuration)

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel signaling on a device, use the **mpls traffic-eng tunnels** command in global configuration mode. To disable MPLS traffic engineering tunnel signaling, use the **no** form of this command.

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables MPLS traffic engineering on a device. For you to use the feature, MPLS traffic engineering must also be enabled on the desired interfaces.

Examples

The following example shows how to turn on MPLS traffic engineering tunnel signaling:

```
Router(config)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
mpls traffic-eng tunnels (interface configuration)	Enables MPLS traffic engineering tunnel signaling on an interface.

mpls traffic-eng tunnels (interface configuration)

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel signaling on an interface (assuming that it is enabled on the device), use the **mpls traffic-eng tunnels** command in interface configuration mode. To disable MPLS traffic engineering tunnel signaling on the interface, use the **no** form of this command.

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enable MPLS traffic engineering on the interface, MPLS traffic engineering must also be enabled on the device. An enabled interface has its resource information flooded into the appropriate IGP link-state database and accepts traffic engineering tunnel signaling requests.

You can use this command to enable MPLS traffic engineering on an interface, thereby eliminating the need to use the **ip rsvp bandwidth** command. However, if your configuration includes CAC (Call Admission Control) for Resource Reservation Protocol (RSVP), you must use the **ip rsvp bandwidth** command.

Examples

The following example shows how to enable MPLS traffic engineering on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
mpls traffic-eng tunnels (global configuration)	Enables MPLS traffic engineering tunnel signaling on a device.

mpls ttl-dec

To specify standard Multiprotocol Label Switching (MPLS) tagging, use the **mpls ttl-dec** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mpls ttl-dec

no mpls ttl-dec

Syntax Description

This command has no arguments or keywords.

Defaults

Optimized MPLS tagging (**no mpls ttl-dec**).

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In Cisco IOS Release 12.2(18)SXE and later releases, MPLS tagging has been optimized to allow the rewriting of the original packet's IP type of service (ToS) and Time to Live (TTL) values before the MPLS label is pushed onto the packet header. This change can result in a slightly lower performance for certain types of traffic. If the packet's original ToS/TTL values are not significant, you enter the **mpls ttl-dec** command for standard MPLS tagging.

Examples

This example shows how to configure the Cisco 7600 series router to use standard MPLS tagging behavior:

```
Router(config)# mpls ttl-dec
Router(config)#
```

This example shows how to configure the Cisco 7600 series router to use optimized MPLS tagging behavior:

```
Router(config)# no mpls ttl-dec
Router(config)#
```

Related Commands

Command	Description
mpls l2transport route	Enables routing of Layer 2 packets over MPLS.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration submode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	MTU size, in bytes.

Defaults

Table 11 lists default MTU values according to media type.

Table 11 Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if)
Connect configuration submode (for Frame Relay Layer 2 interworking)
xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	This command was modified. This command was updated to support connect configuration submode for Frame Relay Layer 2 interworking.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB. Support for this command on the Supervisor Engine 2 was extended to the 12.2SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Release	Modification
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.4	This command was modified. Support for the xconnect subinterface configuration mode was added for this command. The command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies but cannot be set to a value less than 64 bytes.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Changing an MTU size on a Cisco 7500 series router results in the recarving of buffers and resetting of all interfaces. The following message is displayed:

```
%RSP-3-Restart:cbus complex.
```

You can configure native Gigabit Ethernet ports on the Cisco 7200 series router to a maximum MTU size of 9216 bytes. The MTU values range from 1500 to 9216 bytes.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ip mtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, the MTU on a subinterface is equal to the default MTU (4490); if a client is configured, the default is 1500. The MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

Cisco 7600 Valid MTU Values

On the Cisco 7600 platform, valid values are from 64 to 9216 for SVI ports; from 1500 to 9170 for the GE-WAN+ ports; and from 1500 to 9216 for all other ports.

If you enable the jumbo frames, the default is 64 for the SVI ports and 9216 for all the other ports. The jumbo frames are disabled by default.

Cisco uBR10012 Universal Broadband Router

When configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco uBR10012 router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following additional overhead:
  - Layer 2 header—14 bytes

  - Dot1Q header—4 bytes
  - CRC—4 bytes
- If you are using MPLS, be sure that the **mpls mtu** command is configured for a value less than or equal to the interface MTU.
- If you are using MPLS labels, then you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Note For the Gigabit Ethernet SPAs on the Cisco uBR10012 router, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the maximum configurable MTU is 9000 bytes. The SPA automatically adds an additional 22 bytes to the configured MTU size to accommodate some of the additional overhead.

Examples

The following example specifies an MTU of 1000 bytes:

```
Router(config)# interface serial 1
Router(config-if)# mtu 1000
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to specify an MTU size on a Gigabit Ethernet SPA on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# interface GigabitEthernet3/0/0
Router(config-if)# mtu 1800
```

Related Commands

Command	Description
encapsulation smds	Enables SMDS service on the desired interface.
ip mtu	Sets the MTU size of IP packets sent on an interface.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of the BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.

Note Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no** form of the **neighbor activate** command.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The *ipv6-address* argument and support for the IPv6 address family were added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

Examples

Address Exchange Example for Address Family vpn4

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 10.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 10.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 Unicast

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Router(config)# address-family ipv4 unicast
Router(config-router-af)# neighbor group1 activate
Router(config-router-af)# neighbor 172.16.1.1 activate
```

Address Exchange Example for Address Family IPv6

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
exit-address-family	Exits from the address family submode.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor allowas-in

To configure provider edge (PE) routers to allow readvertisement of all prefixes containing duplicate autonomous system numbers (ASNs), use the **neighbor allowas-in** command in router configuration mode. To disable the readvertisement of the ASN of the PE router, use the **no** form of this command.

neighbor *ip-address* **allowas-in** [*number*]

no neighbor allowas-in [*number*]

Syntax Description

ip-address	IP address of the neighboring router.
number	(Optional) Specifies the number of times to allow the advertisement of a PE router's ASN. Valid values are from 1 to 10. If no number is supplied, the default value of 3 times is used.

Command Default

Readvertisement of all prefixes containing duplicate ASNs is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In a hub and spoke configuration, a PE router readvertises all prefixes containing duplicate autonomous system numbers. Use the **neighbor allowas-in** command to configure two VRFs on each PE router to receive and readvertise prefixes are as follows:

- One Virtual Private Network routing and forwarding (VRF) instance receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers.
- The other VRF receives prefixes with ASNs from the customer edge (CE) router and readvertises them to all PE routers in the hub and spoke configuration.

You control the number of times an ASN is advertised by specifying a number from 1 to 10.

Examples

The following example shows how to configure the PE router with ASN 100 to allow prefixes from the VRF address family Virtual Private Network (VPN) IPv4 vrf1. The neighboring PE router with the IP address 192.168.255.255 is set to be readvertised to other PE routers with the same ASN six times.

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf1
Router(config-router)# neighbor 192.168.255.255 allowas-in 6
```

Related Commands

Command	Description
address-family	Enters the address family configuration submode used to configure routing protocols such as BGP, OSPF, RIP, and static routing.

neighbor as-override

To configure a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider, use the **neighbor as-override** command in router configuration mode. To remove Virtual Private Network (VPN) IPv4 prefixes from a specified router, use the **no** form of this command.

neighbor *ip-address* **as-override**

no neighbor *ip-address* **as-override**

Syntax Description

ip-address	Specifies the IP address of the router that is to be overridden with the ASN provided.

Defaults

Automatic override of the ASN is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used in conjunction with the site-of-origin feature, identifying the site where a route originated, and preventing routing loops between routers within a VPN.

Examples

The following example shows how to configure a router to override the ASN of a site with the ASN of a provider:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 192.168.255.255 remote-as 109
Router(config-router)# neighbor 192.168.255.255 update-source loopback0
Router(config-router)# address-family ipv4 vrf vpn1
Router(config-router)# neighbor 192.168.255.255 activate
Router(config-router)# neighbor 192.168.255.255 as-override
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Allows a neighboring router's IP address to be included in the BGP routing table.
neighbor update-source	Allows internal BGP sessions to use any operational interface for TCP/IP connections.
route-map	Redistributes routes from one routing protocol to another.

neighbor inter-as-hybrid

To configure the eBGP peer router (ASBR) as an Inter-AS Option AB peer, use the **neighbor inter-as-hybrid** command.

- Advertised routes have the route targets (RTs) that are configured on the VRF. Advertised routes do not have their original RTs.
- If any prefixes are imported into Option AB VRFs, then the imported paths are advertised to this peer.

neighbor {*ip-address* | *peer-group-name*} **inter-as-hybrid**

no neighbor {*ip-address* | *peer-group-name*} **inter-as-hybrid**

Syntax Description

ip-address	Specifies the IP address of the Inter-AS AB neighbor.
peer-group-name	Specifies the name of a BGP peer group.
inter-as-hybrid	Specifies that the neighbor is an Option AB neighbor.

Defaults

No Inter-AS AB neighbor eBGP (ASBR) router is specified.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was modified. It was integrated into the release.

Examples

The following example specifies an Inter-AS AB neighbor eBGP (ASBR) router:

```
Router(config-router-af)# neighbor 10.0.0.1 inter-as-hybrid
```

Related Commands

Command	Description
address-family vpn4	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
inter-as-hybrid	Specifies a VRF as an Option AB VRF.
neighbor	Adds an entry to the BGP or multiprotocol BGP neighbor table.
neighbor activate	Enables the exchange of information with a neighboring router.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
peer-group-name	Name of a BGP peer group.

Command Default

BGP routers distribute only BGP routes.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	The *ipv6-address* argument was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command enables a router to use BGP to distribute MPLS labels along with the IPv4 routes to a peer router. You must issue this command on both the local router and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the command does not take effect until the BGP session is restarted.
- In router configuration mode, only IPv4 addresses are distributed.

Use this command in IPv6 address family configuration mode to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Cisco IOS installs /32 routes for directly connected external BGP (eBGP) peers when the BGP session for such a peer comes up. The /32 routes are installed only when MPLS labels are exchanged between such peers. Directly connected eBGP peers exchange MPLS labels for:

- IP address families (IPv4 and IPv6) with the **neighbor send-label** command enabled for the peers
- VPN address families (VPNv4 and VPNv6)

A single BGP session can include multiple address families. If one of the families exchanges MPLS labels, the /32 neighbor route is installed for the connected peer.

Examples

The following example shows how to enable a router in the autonomous system 65000 to send MPLS labels with BGP routes to the neighbor BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighbor BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

neighbor send-label explicit-null

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router, use the **neighbor send-label explicit-null** command in address family configuration mode or router configuration mode. To disable a BGP router from sending MPLS labels with explicit-null information, use the **no** form of this command.

neighbor *ip-address* **send-label explicit-null**

no neighbor *ip-address* **send-label explicit-null**

Syntax Description

ip-address	IP address of the neighboring router.

Command Default

None

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command enables a CSC-CE router to use BGP to distribute MPLS labels with a value of zero for explicit-null instead of implicit-null along with IPv4 routes to a CSC-PE peer router.

You must issue this command only on the local CSC-CE router.

You can use this command only with IPv4 addresses.

Examples

In the following CSC-CE example, CSC is configured with BGP to distribute labels and to advertise explicit null for all its connected routes:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# router bgp 100

Router(config-router)# neighbor 10.0.0.2 remote-as 300

Router(config-router)# address-family ipv4
```

```
Router(config-router-af)# neighbor 10.0.0.2 send-label explicit-null
```

In the following CSC-PE example, CSC is configured with BGP to distribute labels:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# router bgp 300

Router(config-router)# neighbor 10.0.0.1 remote-as 100

Router(config-router)# address-family ipv4 vrf v1

Router(config-router-af)# neighbor 10.0.0.1 send-label
```

Note Explicit null is not applicable on a CSC-PE router.

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.

next-address

To specify the next IP address in the explicit path, use the **next-address** command in IP explicit path configuration mode.

next-address [**loose** | **strict**] *ip-address*

Syntax Description

loose	(Optional) Specifies that the previous address (if any) in the explicit path need not be directly connected to the next IP address, and that the router is free to determine the path from the previous address (if any) to the next IP address.
strict	(Optional) Specifies that the previous address (if any) in the explicit path must be directly connected to the next IP address.
ip-address	Next IP address in the explicit path.

Command Default

The next IP address in the explicit path is not specified.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(19)ST1	The **loose** and **strict** keywords were added.
12.0(21)ST	Support for the Cisco 12000 series router was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

To specify an explicit path that includes only the addresses specified, specify each address in sequence by using the **next-address** command without the **loose** keyword.

To configure an interarea traffic engineering (TE) tunnel, configure the tunnel path options as loose explicit paths. Specify that each Autonomous System Boundary Router (ASBR) traversed by the tunnel label switched path (LSP) is a loose hop by entering the **loose** keyword with the **next-address** command.

To use explicit paths for TE tunnels within an Interior Gateway Protocol (IGP) area, you can specify a combination of both loose and strict hops.

When specifying an explicit path for an MPLS TE tunnel, you can specify link or node addresses of the next-hop routers in an explicit path. You can also specify a mixture of link and node addresses. However, there are some restrictions:

- In Cisco IOS Releases 12.2(33)SRD and 12.4(24)T, and Cisco XE Release 2.4 and earlier releases, you cannot specify an explicit path that uses a link address as the first hop and then node addresses as the subsequent hops. However, you can use a node address as the first hop andlink addresses as the subsequent hops.
- In Cisco IOS Releases after 12.2(33)SRD, 12.4(24)T , and Cisco XE Release 2.4, you can use a link address as the first hop and then node addresses as the subsequent hops. There are no restrictions when specifying a mixture of link and node addresses.

When specifying an explicit path, if you specify the "forward" address (the address of the interface that forwards the traffic to the next router) as the next-hop address, the explicit path might not be used. Using the forward address allows that entry to be treated as a loose hop for path calculation. Cisco recommends that you use the "receive"address (the address of the interface that receives traffic from the sending router) as the next-hop address.

In the following example, router R3 sends traffic to router R1. The paths marked a,b and x,y between routers R1 and R2 are parallel paths.

```
R1(a)----(b)R2(c)--(d)R3
  (x)----(y)
```

If you configure an explicit path from R3 to R1 using the "forward" addresses (addresses d and b), the tunnel might reroute traffic over the parallel path (x,y) instead of the explicit path. To ensure that the tunnel uses the explicit path, specify the "receive" addresses as part of the **next-address** command, as shown in the following example:

```
ip explicit-path name path1
  next-address (c)
  next-address (a)
```

Examples

The following example shows how to assign the number 60 to the IP explicit path, enable the path, and specify 10.3.27.3 as the next IP address in the list of IP addresses:

```
Router(config)# ip explicit-path identifier 60 enable
Router(cfg-ip-expl-path)# next-address 10.3.27.3

Explicit Path identifier 60:
    1: next-address 10.3.27.3
```

The following example shows a loose IP explicit path with ID 60. An interarea TE tunnel has a destination of 10.3.29.3 and traverses ASBRs 10.3.27.3 and 10.3.28.3.

```
Router(config)# ip explicit-path identifier 60
Router(cfg-ip-expl-path)# next-address loose 10.3.27.3
Router(cfg-ip-expl-path)# next-address loose 10.3.28.3
Router(cfg-ip-expl-path)# next-address loose 10.3.29.3
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number.
index	Inserts or modifies a path entry at a specified index.
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
show ip explicit-paths	Displays configured IP explicit paths.

oam retry

To configure parameters related to Operation, Administration, and Maintenance (OAM) management for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle, or label-controlled ATM (LC-ATM) VC, use the **oam retry** command in the appropriate command mode. To remove OAM management parameters, use the **no** form of this command.

oam retry *up-count down-count retry-frequency*

no oam retry

Syntax Description

up-count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a connection state to up. This argument does not apply to SVCs.
down-count	Number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change the state to down or tear down an SVC connection.
retry-frequency	The frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *retry-frequency* (in seconds) argument is specified using the **oam-pvc** command, loopback cells are sent at the *retry-frequency* to verify whether the PVC is down.

Defaults

ATM PVCs and SVCs

up-count: 3
down-count: 5
retry-frequency: 1 second

LC-ATM VCs

up-count: 2
down-count: 2
retry-frequency: 2 seconds

Command Modes

Bundle configuration mode (for a VC bundle)
Control-VC configuration (for an LC-ATM VC)
Interface-ATM-VC configuration (for an ATM PVC or SVC)
PVC range configuration (for an ATM PVC range)
PVC-in-range configuration (for an individual PVC within a PVC range)
VC-class configuration (for a VC class)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(3)T	This command was modified to allow configuration parameters related to OAM management for ATM VC bundles.

Release	Modification
12.1(5)T	This command was implemented in PVC range and PVC-in-range configuration modes.
12.3(2)T	This command was implemented in control-VC configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The following guidelines apply to PVCs, SVCs, and VC classes. They do not apply to LC-ATM VCs.

- For ATM PVCs, SVCs, or VC bundles, if the **oam retry** command is not explicitly configured, the VC inherits the following default configuration (listed in order of precedence):
  - Configuration of the **oam retry** command in a VC class assigned to the PVC or SVC itself.
  - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM subinterface.
  - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM main interface.
  - Global default: *up-count* = 3, *down-count* = 5, *retry-frequency* = 1 second. This set of defaults assumes that OAM management is enabled using the **oam-pvc** or **oam-svc** command. The *up-count* and *retry-frequency* arguments do not apply to SVCs.
- To use this command in bundle configuration mode, enter the bundle command to create the bundle or to specify an existing bundle before you enter this command.
- If you use the **oam retry** command to configure a VC bundle, you configure all VC members of that bundle. VCs in a VC bundle are further subject to the following inheritance rules (listed in order of precedence):
  - VC configuration in bundle-vc mode
  - Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
  - Subinterface configuration in subinterface mode

Examples

The following example shows how to configure the OAM management parameters with an up count of 3, a down-count of 3, and the retry frequency set at 10 seconds:

```
Router(cfg-mpls-atm-cvc)# oam retry 3 3 10
```

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
encapsulation	Sets the encapsulation method used by the interface.
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle.
oam-pvc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or virtual circuit class.
oam-svc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM SVC or virtual circuit class.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

oam-ac emulation-enable

To enable Operation, Administration, and Maintenance (OAM) cell emulation on ATM adaptation layer 5 (AAL5) over Multiprotocol Label Switching (MPLS) or Layer 2 Tunnel Protocol Version 3 (L2TPv3), use the **oam-ac emulation-enable** command in the appropriate configuration mode on both provider edge (PE) routers. To disable OAM cell emulation, use the **no** form of this command on both routers.

oam-ac emulation-enable [*seconds*]

no oam-ac emulation-enable [*seconds*]

Syntax Description

seconds	(Optional) The rate (in seconds) at which the alarm indication signal (AIS) cells should be sent. The range is 0 to 60 seconds. If you specify 0, no AIS cells are sent. The default is 1 second, which means that one AIS cell is sent every second.

Command Default

OAM cell emulation is disabled.

Command Modes

L2transport VC configuration—for an ATM PVC
VC class configuration mode—for a VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable OAM cell emulation as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is used with AAL5 over MPLS or L2TPv3 and is not supported with ATM cell relay over MPLS or L2TPv3.

Examples

The following example shows how to enable OAM cell emulation on an ATM permanent virtual circuit (PVC):

```
Router# interface ATM 1/0/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable
```

The following example shows how to set the rate at which an AIS cell is sent every 30 seconds:

```
Router# interface ATM 1/0/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30
```

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.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm oamclass
Router(config-vc-class)# encapsulation aal5
Router(config-vc-class)# oam-ac emulation-enable 30
Router(config-vc-class)# oam-pvc manage
Router(config)# interface atm1/0
Router(config-if)# class-int oamclass
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.

oam-pvc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC), virtual circuit (VC) class, or label-controlled ATM (LC-ATM) VC, use the **oam-pvc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

ATM VC or VC Class

oam-pvc [**manage**] [*frequency*]

no oam-pvc [**manage**]

LC-ATM VC

oam-pvc manage [*frequency*]

no oam-pvc manage

Loopback Mode Detection

oam-pvc manage [*frequency*] **loop-detection**

no oam-pvc manage loop-detection

Cisco 10000 Series Router

oam-pvc manage [*frequency*] [**auto-detect** [**optimum**]] [**keep-vc-up** [**seg aisrdi failure**]]

no oam-pvc manage [*frequency*] [**auto-detect** [**optimum**]] [**keep-vc-up** [**seg aisrdi failure**]]

Syntax Description

manage	(Optional for ATM VCs or VC classes; required for LC-ATM VCs) Enables OAM management. The default is disabled.
frequency	(Optional) Specifies the time delay between transmitting OAM loopback cells, in seconds. For ATM VCs or VC classes and loopback mode detection, the range is from 0 to 600, and the default is 10. For LC-ATM VCs, the range is from 0 to 255, and the default is 5.
loop-detection	Enables automatic detection of whether the physically connected ATM switch is in loopback mode. The default is disabled.
auto-detect	(Optional) Enables auto-detection of peer OAM command cells.
optimum	(Optional) Configures an optimum mode so that when the traffic-monitoring timer expires, the PVC sends an OAM command cell at the locally configured frequency instead of going into Retry mode immediately. If there is no response, the PVC goes into Retry mode.
keep-vc-up	(Optional) Specifies that the VC will be kept in the UP state when continuity check (CC) cells detect connectivity failure.
seg aisrdi failure	(Optional) Specifies that if segment alarm indication signal/remote defect indication (AIS/RDI) cells are received, the VC will not be brought down because of end CC failure or loopback failure.

Command Default OAM management and loop detection are disabled.

Command Modes
ATM VC class configuration (for a VC class)
ATM VC configuration (for an ATM PVC or loopback mode detection)
Control-VC configuration (for enabling OAM management on an LC-ATM VC)
PVC-in-range configuration (for an individual PVC within a PVC range)

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was implemented in PVC-in-range configuration mode.
12.3(2)T	This command was implemented for LC-ATM VCs.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S, and the **loop-detection** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines If OAM management is enabled, further control of OAM management is configured by using the **oam retry** command.

ATM VC or VC Classes

If the **oam-pvc** command is not explicitly configured on an ATM PVC, the PVC inherits the following default configuration (in order of precedence):

- Configuration from the **oam-pvc** command in a VC class assigned to the PVC itself.
- Configuration from the **oam-pvc** command in a VC class assigned to the ATM subinterface of the PVC.
- Configuration from the **oam-pvc** command in a VC class assigned to the ATM main interface of the PVC.
- Global default: End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back. The default value for the *frequency* argument is 10 seconds.

Loopback Mode Detection

When a PVC traverses an ATM cloud and OAM is enabled, the router sends a loopback cell to the other end and waits for a response to determine whether the circuit is up. If an intervening router within the ATM cloud is in loopback mode, however, the router considers the circuit to be up, when in fact the other end is not reachable.

When enabled, the Loopback Mode Detection Through OAM feature detects when an intervening router is in loopback mode, in which case it sets the OAM state to NOT_VERIFIED. This prevents traffic from being routed on the PVC for as long as any intervening router is detected as being in loopback mode.

Examples

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an ATM PVC with a transmission frequency of 3 seconds:

```
Router(cfg-mpls-atm-cvc)# oam-pvc manage 3
```

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an LC-ATM interface with a transmission frequency of 2 seconds:

```
Router(config)# interface Switch1.10 mpls
Router(config-subif)# ip unnumbered Loopback0
Router(config-subif)# mpls atm control-vc 0 32
Router(cfg-mpls-atm-cvc)# oam-pvc manage 2
```

The following example shows how to create a PVC and enable loopback detection:

```
Router(config)# interface ATM1/0
Router(config-if)# pvc 4/100
Router(config-if-atm-vc)# oam-pvc manage loop-detection
```

Related Commands

Command	Description
ilmi manage	Enables ILMI management on an ATM PVC.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or LC-ATM VC.
show atm pvc	Displays all ATM PVCs and traffic information.

ping mpls

To check Multiprotocol Label Switching (MPLS) label switched path (LSP) connectivity, use the **ping mpls** command in privileged EXEC mode.

ping mpls {**ipv4** *destination-address*/*destination-mask-length* [**destination** *address-start address-end increment*] [**ttl** *time-to-live*] | **pseudowire** *ipv4-address vc-id* [**segment** [*segment-number*]] [**destination** *address-start address-end increment*] | **traffic-eng** *tunnel-interface tunnel-number* [**ttl** *time-to-live*]}
[**revision** {**1** | **2** | **3** | **4**}]
[**source** *source-address*]
[**repeat** *count*]
[**timeout** *seconds*]
[**size** *packet-size* | **sweep** *minimum maximum size-increment*]
[**pad** *pattern*]
[**reply dscp** *dscp-value*]
[**reply pad-tlv**]
[**reply mode** {**ipv4** | **router-alert**}]
[**interval** *ms*]
[**exp** *exp-bits*]
[**verbose**]
[**revision** *tlv-revision-number*]
[**force-explicit-null**]
[**output interface** *tx-interface* [**nexthop** *ip-address*]]
[**dsmap** [**hashkey** {**none** | **ipv4 bitmap** *bitmap-size*}]]
[**flags fec**]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
destination-address	Address prefix of the target to be tested.
/destination-mask-length	Number of bits in the network mask of the target address. The slash is required.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) Beginning network 127 address.
address-end	(Optional) Ending network 127 address.
increment	(Optional) Number by which to increment the network 127 address.
ttl *time-to-live*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.
pseudowire	Specifies the destination type as an Any Transport over MPLS (AToM) virtual circuit (VC).
ipv4-address	IPv4 address of the AToM VC to be tested.
vc-id	Specifies the VC identifier of the AToM VC to be tested.
segment *segment-number*	(Optional) Specifies a segment of a multisegment pseudowire.
traffic-eng	Specifies the destination type as an MPLS traffic engineering (TE) tunnel.
tunnel-interface	Tunnel interface to be tested.
tunnel-number	Tunnel interface number.

revision {**1** | **2** | **3** | **4**}	(Optional) Selects the type, length, values (TLVs) version of the implementation. Use the **revision 4** default unless attempting to interoperate with devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2. If you do not select a **revision** keyword, the software uses the latest version. See Table 12 in the "Revision Keyword Usage" section of the "Usage Guidelines" section for information on when to select the **1**, **2**, **3**, and **4** keywords.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
repeat *count*	(Optional) Specifies the number of times to resend the same packet. The range is from 1 to 2147483647. The default is 1. If you do not enter the **repeat** keyword, the software resends the same packet five times.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is from 0 to 3600. The default is 2 seconds.
size *packet-size*	(Optional) Specifies the size of the packet with the label stack imposed. Packet size is the number of bytes in each ping. The range is from 40 to 18024. The default is 100.
sweep	(Optional) Enables you to send a number of packets of different sizes, ranging from a start size to an end size. This parameter is similar to the Internet Control Message Protocol (ICMP) **ping sweep** parameter.
minimum	(Optional) Minimum or start size for an MPLS echo packet. The lower boundary of the **sweep** range varies depending on the LSP type. The default is 100 bytes.
maximum	(Optional) Maximum or end size for an echo packet. The default is 17,986 bytes.
size-increment	(Optional) Number by which to increment the echo packet size. The default is 100 bytes.
pad *pattern*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
reply dscp *dscp-value*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
reply pad-tlv	(Optional) Tests the ability of the sender of an echo reply to support the copy pad TLV to echo reply.
reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. **ipv4**—Reply with an IPv4 UDP packet (default). **router-alert**—Reply with an IPv4 UDP packet with router alert.
interval *ms*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving router does not drop packets. Default is 0.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.

verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
dsmap	(Optional) Interrogates a transit router for downstream mapping (DSMAP) information.
hashkey {**none** | **ipv4 bitmap** *bitmap-size*}	(Optional) Allows you to control the hash key and multipath settings. Valid values are: **none**—There is no multipath (type 0). **ipv4 bitmap** *bitmap-size*—Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Be sure to use this keyword in conjunction with the **ttl** keyword.

Command Default

You cannot check MPLS LSP connectivity.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	The **reply dscp** and **reply pad-tlv** keywords were added.
12.4(6)T	The following keywords were added: **revision**, **force-explicit-null**, **output interface**, **dsmap**, **hashkey**, **none**, **ipv4 bitmap**, and **flags fec**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **nexthop** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Release	Modification
Cisco IOS XE Release 2.3	This command was updated with the **segment** keyword.
12.2(33)SRE	This command was modified. Restrictions were added to the **pseudowire** keyword.

Usage Guidelines

Note It is recommended that you use the **mpls oam** global configuration command instead of this command.

Use the **ping mpls** command to validate, test, or troubleshoot IPv4 LDP LSPs, IPv4 Resource Reservation Protocol (RSVP) TE tunnels, and AToM VCs.

UDP Destination Address Usage

The destination address is a valid 127/8 address. You have the option to specify a single *x.y.z-address* or a range of numbers from 0.0.0 to *x.y.z*, where *x*, *y*, and *z* are numbers from 0 to 255 and correspond to the 127.*x.y.z* destination address.

The MPLS echo request destination address in the UDP packet is not used to forward the MPLS packet to the destination router. The label stack that is used to forward the echo request routes the MPLS packet to the destination router. The 127/8 address guarantees that the packets are routed to the local host (the default loopback address of the router processing the address) if the UDP packet destination address is used for forwarding.

In addition, the destination address is used to adjust load balancing when the destination address of the IP payload is used for load balancing.

Time-to-Live Usage

The time-to-live value indicates the maximum number of hops a packet should take to reach its destination. The value in the TTL field in a packet is decremented by 1 each time the packet travels through a router.

For MPLS LSP ping, the TTL is a value after which the packet is discarded and an MPLS echo reply is sent back to the originating router.

For MPLS multipath LSP traceroute, the TTL is a maximum time-to-live value and is used to discover the number of downstream hops to the destination router. MPLS LSP traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4, ...) to accomplish this.

Downstream Map TLVs

The presence of a downstream map in an echo request is interpreted by the responding transit (not egress) router to include downstream map information in the echo reply. Specify the **ttl** and **dsmap** keywords to cause TTL expiry during LSP ping to interrogate a transit router for downstream information.

Pseudowire Usage

The following keywords are not available with the **ping mpls pseudowire** command:

- **dsmap**
- **flags**
- **force-explicit-null**

- **output**
- **revision**
- **ttl**

Revision Keyword Usage

The **revision** keyword allows you to issue a **ping mpls ipv4**, **ping mpls pseudowire**, or **trace mpls traffic-eng** command based on the format of the TLV. Table 12 lists the revision option and usage guidelines for each option.

Table 12 Revision Options and Option Usage Guidelines

Revision Option	Option Usage Guidelines
1[1]	Not supported in Cisco IOS Release 12.4(11)T or later releases. Version 1 (draft-ietf-mpls-ping-03). For a device running Cisco IOS Release 12.0(27)S3 or a later release, you must use the **revision 1** keyword when you send LSP ping or LSP traceroute commands to devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2.
2	Version 2 functionality was replaced by Version 3 functionality before an image was released.
3	Version 3 (draft-ietf-mpls-ping-03). • For a device implementing Version 3 (Cisco IOS Release 12.0(27)S3 or a later release), you must use the **revision 1** keyword when you send the LSP **ping** or LSP **traceroute** command to a device implementing Version 1 (that is, either Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2). • A **ping mpls pseudowire** command does not work with devices running Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2.
4	• Version 8 (draft-ietf-mpls-ping-08)—Applicable before Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in Version 8. • RFC 4379 compliant—Applicable after Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in RFC 4379. This is the recommended version.

1. If you do not specify a **revision** keyword, the software uses the latest version.

Examples

The following example shows how to use the **ping mpls** command to test connectivity of an IPv4 LDP LSP:

```
Router# ping mpls ipv4 10.131.191.252/32 repeat 5 exp 5 verbose

Sending 5, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 100/102/112 ms
```

The following example shows how to invoke the **ping mpls** command in the interactive mode to check MPLS LSP connectivity:

```
Router# ping

Protocol [ip]: mpls
Target IPv4, pseudowire or traffic-eng [ipv4]: ipv4
Target IPv4 address: 10.131.159.252
Target mask: 255.255.255.255
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Send interval in msec [0]:
Extended commands? [no]: yes
Destination address or destination start address: 127.0.0.1
Destination end address: 127.0.0.1
Destination address increment: 0.0.0.1
Source address:
EXP bits in mpls header [0]:
Pad TLV pattern [ABCD]:
Time To Live [255]:
Reply mode ( 2-ipv4 via udp, 3-ipv4 via udp with router alert) [2]:
Reply ip header DSCP bits [0]:
Verbose mode? [no]: yes
Sweep range of sizes? [no]:
Sending 1, 100-byte MPLS Echos to 10.131.159.252/32,
      timeout is 2 seconds, send interval is 0 msec:

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
Destination address 127.0.0.1
!   10.131.159.245, return code 3


Destination address 127.0.0.1
!   10.131.159.245, return code 3


Destination address 127.0.0.1
!   10.131.159.245, return code 3


Success rate is 100 percent (3/3), round-trip min/avg/max = 40/48/52 ms
```

Note The "Destination end address" and "Destination address increment" prompts display only if you enter an address at the "Destination address or destination start address" prompt. Also, the "Sweep min size," "Sweep max size," and "Sweep interval" prompts display only if you enter "yes" at the "Sweep range of sizes? [no]" prompt.

The following example shows how to determine the destination address of an AToM VC:

```
Router# show mpls l2transport vc

Local intf     Local circuit           Dest address    VC ID      Status
-------------  ----------------------- --------------- ---------- ----------
Et2/0          Ethernet                10.131.191.252  333        UP

Router# show mpls l2transport vc detail

Local interface: Et2/0 up, line protocol up, Ethernet up
  Destination address: 10.131.191.252, VC ID: 333, VC status: up
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop 10.131.159.246
    Output interface: Et1/0, imposed label stack {16}
  Create time: 06:46:08, last status change time: 06:45:51
  Signaling protocol: LDP, peer 10.131.191.252:0 up
    MPLS VC labels: local 16, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    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
```

This **ping mpls** command used with the **pseudowire** keyword can be used to test the connectivity of the AToM VC 333 discovered in the preceding **show** command:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 200 size 1400

Sending 1, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 92/92/92 ms
```

This ping is particularly useful because the VC might be up and the LDP session between the PE and its downstream neighbor might also be up, but LDP might be configured somewhere in between. In such cases, you can use an LSP ping to verify that the LSP is actually up.

A related point concerns the situation when a pseudowire has been configured to use a specific TE tunnel. For example:

```
Router# show running-config interface ethernet 2/0
```

```
Building configuration...

Current configuration : 129 bytes
!
interface Ethernet2/0
 no ip address
 no ip directed-broadcast
 no cdp enable
xconnect 10.131.191.252 333 pw-class test1
end


Router# show running-config | begin pseudowire

pseudowire-class test1
 encapsulation mpls
 preferred-path interface Tunnel0
!
```

In such cases, you can use an LSP ping to verify the connectivity of the LSP that a certain pseudowire is taking, be it LDP based or a TE tunnel:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 200 size 1400

Sending 200, 1400-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (200/200), round-trip min/avg/max = 72/85/112 ms
```

You can also use the **ping mpls** command to verify the maximum packet size that can be successfully sent. The following command uses a packet size of 1500 bytes:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 5 size 1500

Sending 5, 1500-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
QQQQQ
Success rate is 0 percent (0/5)
```

The Qs indicate that the packets are not sent.

The following command uses a packet size of 1476 bytes:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 5 size 1476
```

```
Sending 5, 1476-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/83/92 ms
```

The following example shows how to test the connectivity of an MPLS TE tunnel:

```
Router# ping mpls traffic-eng tunnel tun3 repeat 5 verbose

Sending 5, 100-byte MPLS Echos to Tunnel3,
     timeout is 2 seconds, send interval is 0 msec:

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0


Type escape sequence to abort.
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/40 ms
```

The MPLS LSP ping feature is useful if you want to verify TE tunnels before actually mapping traffic onto them.

The following example shows a **ping mpls** command that specifies segment 2 of a multisegment pseudowire:

```
Router# ping mpls pseudowire 10.131.191.252 333 segment 2
```

Related Commands

Command	Description
mpls oam	Customizes the default behavior of echo packets.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

preferred-path

To specify the path that traffic uses (a Multiprotocol Label Switching (MPLS) Traffic engineering (TE) tunnel or destination IP address and Domain Name Server (DNS) name), use the **preferred-path** command in pseudowire configuration mode. To disable tunnel selection, use the **no** form of this command.

preferred-path {**interface tunnel** *tunnel-number* | **peer** {*ip-address* | *host-name*}} [**disable-fallback**]

no preferred-path {**interface tunnel** *tunnel-number* | **peer** {*ip-address* | *host-name*}} [**disable-fallback**]

Syntax Description

interface tunnel *tunnel-number*	Specifies an MPLS TE tunnel interface that is the core-facing output interface.
peer *ip-address* | *host-name*	Specifies an IP address or DNS name configured on the peer provider edge (PE) router, which is reachable through a label switched path (LSP).
disable-fallback	(Optional) Disables the router from using the default path when the preferred path is unreachable.

Command Default

Tunnel selection is not enabled.

Command Modes

Pseudowire configuration

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The following guidelines provide more information about using this command:

- The destination IP address can be different from the peer router ID used in MPLS Label Distribution Protocol (LDP). For example, a peer PE router can have multiple loopback IP addresses, which can be reached by different paths, such as a TE tunnel, static IP route, or Interior Gateway Protocol (IGP) route.
- This command is available only if the pseudowire encapsulation type is MPLS.
- Tunnel selection is enabled when you exit from pseudowire configuration mode.
- The selected path should be an LSP destined to the peer PE router.
- The selected tunnel must be an MPLS traffic engineering 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. The address must have a /32 mask.

Examples

The following example creates a pseudowire class and specifies tunnel 1 as the preferred path:

```
Router(config)# pseudowire-class pw1
Router(config-pw)# encapsulation mpls
Router(config-pw)# preferred-path interface tunnel 1 disable-fallback
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

priority (LSP Attributes)

To specify the label switched path (LSP) priority in an LSP attribute list, use the **priority** command in LSP Attributes configuration mode. To remove the specified priority, use the **no** form of this command.

priority *setup-priority* [*hold-priority*]

no priority

Syntax Description

setup-priority	Priority used when signaling an LSP to determine which existing LSPs can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
hold-priority	(Optional) Priority associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

Command Default

No priority is set in the attribute list.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure setup and hold priority for an LSP in an LSP attribute list. Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

To associate the LSP priority attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set the LSP hold and setup property to 0 in an LSP attribute list identified by the string hipriority:

```
configure terminal
!
mpls traffic-eng lsp attributes hipriority
 priority 0 0
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

protection (LSP Attributes)

To configure failure protection on the label switched path (LSP) in an LSP attribute list, use the **protection** command in LSP Attributes configuration mode. To disable failure protection, use the **no** form of this command.

protection fast-reroute

no protection

Syntax Description

fast-reroute	Enables an LSP to use an established backup LSP in the event of a link failure.

Command Default

Failure protection is not enabled for the LSP in the LSP attribute list.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up LSP failure protection in an LSP attribute list.

To associate the LSP failure protection attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to enable failure protection on an LSP in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes protect
 protection fast-reroute
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

protection local-prefixes

To enable PE-CE link protection by preserving the local label (due to a link failure that caused BGP to begin reconverging), use the **protection local-prefixes** command. To disable this form of link protection, use the **no** form of this command:

[no] protection local-prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

This protection is disabled by default.

Command Modes

VRF configuration (config-vrf).

Address-family configuration (config-vrf-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.0(1)M	This command was modified. It was integrated into the release.

Usage Guidelines

- If your Cisco IOS version includes support for IPv6, use the global configuration **vrf definition** command first, followed by the **rd** and **address-family ipv4** commands before you use the **protection local-prefixes** command. If your Cisco IOS version only supports IPv4, use the global configuration **ip vrf** command before you enter the **rd** and **protection local-prefixes** commands. In both cases, use the **rd** command to specify a route distinguisher for the VRF if none has been created previously.
- If VRF-lite has already been enabled, local protection will not take place. This is true even if entering the **protection local-prefixes** command does not trigger an error message.
- Local link protection will only work properly if the failure is quickly detected and an alternate, back-up route already exists. Therefore, in addition to the **protection local-prefixes** command, the use of Bidirectional Forwarding Detection (BFD) and topology-specific routing protocols are both required.

Examples

The following example enables local protection in an IPv6-supporting version of Cisco IOS, using the only supported (IPv4) option:

```
vrf definition vrf2
rd 100:3
address-family ipv4
protection local prefixes
```

The following example enables local protection in an IPv4-only version of Cisco IOS:

```
ip vrf vpn1
rd 100:3
protection local prefixes
```

Related Commands

Command	Description
bfd interval min_rx multiplier	Enables BFD on the interface.
neighbor fall-over bfd	Enables BFD support for fallover.

pseudowire

To bind an attachment circuit to a Layer 2 pseudowire for xconnect service, use the **pseudowire** command in interface configuration mode.

pseudowire *peer-ip-address vcid* **pw-class** *pw-class-name* [**sequencing** {**transmit** | **receive** | **both**}]

Syntax Description

peer-ip-address	The IP address of the remote peer.
vcid	The 32-bit identifier of the virtual circuit between the routers at each end of the Layer 2 control channel.
pw-class *pw-class-name*	The pseudowire class configuration from which the data encapsulation type will be taken.
sequencing {**transmit** | **receive** | **both**}	(Optional) Sets the sequencing method to be used for packets received or sent in L2TP sessions: • **transmit**—Sequencing of Layer 2 Tunnel Protocol (L2TP) data packets received from the session. • **receive**—Sequencing of L2TP data packets sent into the session. • **both**—Sequencing of L2TP data packets that are both sent and received from the session.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each pseudowire configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

The same *vcid* value that identifies the attachment circuit must be configured using the **pseudowire** command on the local and remote router at each end of a Layer 2 session. The virtual circuit identifier creates the binding between a pseudowire and an attachment circuit.

The **pw-class** *pw-class-name* value binds the pseudowire configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **pseudowire** command.

Examples

The following example creates a virtual-PPP interface with the number 1, configures PPP on the virtual-PPP interface, and binds the attachment circuit to a Layer 2 pseudowire for xconnect service for the pseudowire class named pwclass1:

```
interface virtual-ppp 1
 ppp authentication chap
 ppp chap hostname peer1
 pseudowire 172.24.13.196 10 pw-class pwclass1
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

pseudowire-class

To specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class [*pw-class-name*]

no pseudowire-class [*pw-class-name*]

Syntax Description

pw-class-name	(Optional) The name of a Layer 2 pseudowire class. If you want to configure more than one pseudowire class, you must enter a value for the *pw-class-name* argument.

Command Default

No pseudowire classes are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The **pseudowire-class** command allows you to configure a pseudowire class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- Sequencing
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

After you enter the **pseudowire-class** command, the router switches to pseudowire class configuration mode, where pseudowire settings may be configured.

Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named “ether-pw”:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)#
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd** command in VRF configuration submode.

rd *route-distinguisher*

Syntax Description

route-distinguisher	Adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

There is no default. An RD must be configured for a VRF to be functional.

Command Modes

VRF configuration submode

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN-related—Composed of an autonomous system number and an arbitrary number.
- IP-address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

*16-bit autonomous-system-number***:***your 32-bit number*
For example, 101:3.

*32-bit IP address***:***your 16-bit number*
For example, 192.168.122.15:1.

Examples

The following example shows how to configure a default RD for two VRFs. It illustrates the use of both autonomous-system-number-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router (config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

record-route (LSP Attributes)

To record the route used by the label switched path (LSP), use the **record-route** command in LSP Attributes configuration mode. To stop the recording the route used by the LSP, use the **no** form of this command.

record-route

no record-route

Syntax Description

This command has no arguments or keywords.

Command Default

The LSP route is not recorded.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up in an LSP attribute list the recording of the route taken by the LSP.

To associate the LSP record-route attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set up LSP route recording in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes 9
 record-route
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **route-target** command in VRF configuration submode. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target {**import** | **export** | **both**} *route-target-ext-community*

no route-target {**import** | **export** | **both**} *route-target-ext-community*

Syntax Description

import	Imports routing information from the target VPN extended community.
export	Exports routing information to the target VPN extended community.
both	Imports both import and export routing information to the target VPN extended community.
route-target-ext-community	Adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.

Command Default

A VRF has no route-target extended community attributes associated with it until specified by the **route-target** command.

Command Modes

VRF configuration submode (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.

Usage Guidelines

The **route-target** command creates lists of import and export route target extended communities for the specified VRF. Enter the command one time for each target community. Learned routes that carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target. Routes learned from a VRF site (for example, by Border Gateway Protocol (BGP), Routing Information Protocol (RIP), or static route configuration) contain export route targets for extended communities configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route target specifies a target VPN extended community. Like a route-distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

- *16-bit autonomous-system-number*:*your 32-bit number*
  For example, 101:3.
- *32-bit IP address*:*your 16-bit number*
  For example, 192.168.122.15:1.

In Cisco IOS Release 12.0(32)SY8, 12.2(33)SXI1, 12.0(33)S3, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example shows how to configure route-target extended community attributes for a VRF in IPv4. The result of the command sequence is that VRF named vrf1 has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 10.27.0.130:200):

```
ip vrf vrf1
 route-target both 1000:1
 route-target export 1000:2
 route-target import 10.27.0.130:200
```

The following example shows how to configure route-target extended community attributes for a VRF that includes IPv4 and IPv6 address families:

```
vrf definition site1
rd 1000:1
```

```
address-family ipv4
 route-target export 100:1
 route-target import 100:1
address-family ipv6
 route-target export 200:1
 route-target import 200:1
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.2(33)SXI1, 12.0(33)S3, Cisco IOS XE Release 2.4, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number in asplain format—65537—and how to set the route-target to extended community value 65537:100 for routes that are permitted by the route map.

```
ip vrf vpn_red
 rd 64500:100
 route-target both 65537:100
 exit
route-map red_map permit 10
 set extcommunity rt 65537:100
 end
```

After the configuration is completed, use the **show route-map** command to verify that the extended community is set to the route target containing the 4-byte autonomous system number of 65537.

```
Router# show route-map red_map

route-map red_map, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number in asdot format—1.1—and how to set the route-target to extended community value 1.1:100 for routes that are permitted by the route map.

```
ip vrf vpn_red
 rd 64500:100
 route-target both 1.1:100
 exit
route-map red_map permit 10
 set extcommunity rt 1.1:100
 end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

sequencing

To configure the direction in which sequencing is enabled for data packets in a Layer 2 pseudowire, use the **sequencing** command in pseudowire class configuration mode. To remove the sequencing configuration from the pseudowire class, use the **no** form of this command.

sequencing {**transmit** | **receive** | **both** | **resync** *number*}

no sequencing {**transmit** | **receive** | **both** | **resync** *number*}

Syntax Description

transmit	Updates the Sequence Number field in the headers of data packets sent over the pseudowire according to the data encapsulation method that is used.
receive	Keeps the value in the Sequence Number field in the headers of data packets received over the pseudowire. Out-of-order packets are dropped.
both	Enables both the **transmit** and **receive** options.
resync	Enables the reset of packet sequencing after the disposition router receives a specified number of out-of-order packets.
number	The number of out-of-order packets that cause a reset of packet sequencing. The range is 5 to 65535.

Command Default

Sequencing is disabled.

Command Modes

Pseudowire class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced for Layer 2 Tunnel Protocol Version 3 (L2TPv3).
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.0(29)S	This command was updated to support Any Transport over MPLS (AToM).
12.0(30)S	The **resync** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	L2TPv3 support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	AToM support for this command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

When you enable sequencing using any of the available options, the sending of sequence numbers is automatically enabled and the remote provider edge (PE) peer is requested to send sequence numbers. Out-of-order packets received on the pseudowire are dropped only if you use the **sequencing receive** or **sequencing both** command.

If you enable sequencing for Layer 2 pseudowires on the Cisco 7500 series routers and you issue the **ip cef distributed** command, all traffic on the pseudowires is switched through the line cards.

It is useful to specify the **resync** keyword for situations when the disposition router receives many out-of-order packets. It allows the router to recover from situations where too many out-of-order packets are dropped.

Examples

The following example shows how to enable sequencing in data packets in Layer 2 pseudowires that were created from the pseudowire class named "ether-pw" so that the Sequence Number field is updated in tunneled packet headers for data packets that are both sent and received over the pseudowire:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation mpls
Router(config-pw)# sequencing both
```

The following example shows how to enable the disposition router to reset packet sequencing after it receives 1000 out-of-order packets:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation mpls
Router(config-pw)# sequencing both
Router(config-pw)# sequencing resync 1000
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the Route Processor card.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

set extcomm-list delete

To allow the deletion of extended community attributes based on an extended community list, use the **set extcomm-list delete** command in route-map configuration mode. To negate a previous **set extcomm-list detect** command, use the **no** form of this command.

set extcomm-list *extended-community-list-number* **delete**

no set extcomm-list *extended-community-list-number* **delete**

Syntax Description

extended-community-list-number	An extended community list number.

Command Default

Extended community attributes based on an extended community list cannot be deleted.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command removes extended community attributes of an inbound or outbound Border Gateway Protocol (BGP) update using a route map to filter and determine the extended community attribute to be deleted and replaced. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each extended community that passes the route map permit clause and matches the given extended community list will be removed and replaced from the extended community attribute being received from or sent to the BGP neighbor.

Examples

The following example shows how to replace a route target 100:3 on an incoming update with a route target of 100:4 using an inbound route map extmap:

```
.
.
.
Router(config-af)# neighbor 10.10.10.10 route-map extmap in
.
.
.
Router(config)# ip extcommunity-list 1 permit rt 100:3
Router(config)# route-map extmap permit 10
Router(config-route-map)# match extcommunity 1
Router(config-route-map)# set extcomm-list 1 delete
Router(config-route-map)# set extcommunity rt 100:4 additive
```

The following example shows how to configure more than one replacement rule using the route-map configuration **continue** command. Prefixes with RT 100:2 are rewritten to RT 200:3 and prefixes with RT 100:4 are rewritten to RT 200:4. With the **continue** command, route-map evaluation proceeds even if a match is found in a previous sequence.

```
Router(config)# ip extcommunity-list 1 permit rt 100:3
Router(config)# ip extcommunity-list 2 permit rt 100:4
Router(config)# route-map extmap permit 10
Router(config-route-map)# match extcommunity 1
Router(config-route-map)# set extcomm-list 1 delete
Router(config-route-map)# set extcommunity rt 200:3 additive
Router(config-route-map)# continue 20
Router(config)# route-map extmap permit 20
Router(config-route-map)# match extcommunity 2
Router(config-route-map)# set extcomm-list 2 delete
Router(config-route-map)# set extcommunity rt 200:4 additive
Router(config-route-map)# exit
Router(config)# route-map extmap permit 30
```

Related Commands

Command	Description
ip community-list	Creates an extended community access list and controls access to it.
match extcommunity	Matches BGP extended community list attributes.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set extcommunity	Sets BGP extended community attributes.

set mpls experimental

To set the Multiprotocol Label Switching (MPLS) experimental-bit value, use the **set mpls experimental** command in QoS policy-map configuration mode. To return to the default settings, use the **no** form of this command.

set mpls experimental {**imposition** | **topmost**} *experimental-value*

no set mpls experimental {**imposition** | **topmost**}

Syntax Description

imposition	Specifies the experimental-bit value on IP to Multiprotocol Label Switching (MPLS) or MPLS input in all newly imposed labels.
topmost	Specifies the experimental-bit value on the topmost label on the input or output flows.
experimental-value	Experimental-bit value; valid values are from 0 to 7.

Defaults

No experimental-bit value is set.

Command Modes

QoS policy-map configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine 2.

Examples

This example shows how to set the experimental-bit value on the topmost label on input or output:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set mpls experimental topmost 5
```

set mpls experimental imposition

To set the value of the Multiprotocol Label Switching (MPLS) experimental (EXP) field on all imposed label entries, use the **set mpls experimental imposition** command in QoS policy-map class configuration mode. To disable the setting, use the **no** form of this command.

set mpls experimental imposition {*mpls-exp-value* | *from-field* [**table** *table-map-name*]}

no set mpls experimental imposition {*mpls-exp-value* | *from-field* [**table** *table-map-name*]}

Cisco 10000 Series Router

set mpls experimental imposition *mpls-exp-value*

no set mpls experimental imposition *mpls-exp-value*

Syntax Description

mpls-exp-value	Specifies the value used to set MPLS EXP bits defined by the policy map. Valid values are numbers from 0 to 7.
from-field	Specific packet-marking category to be used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows: • **precedence** • **dscp**
table	(Optional) Used in conjunction with the *from-field* argument. Indicates that the values set in a specified table map will be used to set the MPLS EXP imposition value.
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the MPLS EXP imposition value. The name can be a maximum of 64 alphanumeric characters.

Defaults

No MPLS EXP value is set.

Command Modes

QoS policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced; it replaces (renames) the **set mpls experimental** command, introduced in 12.1(5)T. The **set mpls experimental imposition** command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.3(7)XII	This command was implemented on the ESR–PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **set mpls experimental imposition** command is supported only on input interfaces. Use this command during label imposition. This command sets the MPLS EXP field on all imposed label entries.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the class of service (CoS) value. The "from-field" packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the "from-field" category as the MPLS EXP imposition value. For instance, if you configure the **set mpls experimental imposition precedence** command, the precedence value will be copied and used as the MPLS EXP imposition value.

If you configure the **set mpls experimental imposition dscp** command, the DSCP value will be copied and used as the MPLS EXP imposition value.

Note If you configure the **set mpls experimental imposition dscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

Cisco 10000 Series Router

Cisco IOS software replaced the **set mpls experimental** command with the **set mpls experimental imposition** command. However, the Cisco 10000 series router continues to use the **set mpls experimental** command for ESR–PRE1. For ESR–PRE2, the command is **set mpls experimental imposition**.

Examples

The following example shows how to set the MPLS EXP value to 3 on all imposed label entries:

```
Router(config-pmap-c)# set mpls experimental imposition 3
```

The following example shows how to create the policy map named policy1 to use the packet-marking values defined in a table map named table-map1. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page. The MPLS EXP imposition value is set according to the DSCP value defined in table-map1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set mpls experimental imposition dscp table table-map1
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost label on either an input or an output interface.
set precedence	Sets the precedence value in the packet header.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set mpls experimental topmost

To set the Multiprotocol Label Switching (MPLS) experimental (EXP) field value in the topmost label on either an input or an output interface, use the **set mpls experimental topmost** command in QoS policy-map class configuration mode. To disable the setting, use the **no** form of this command.

set mpls experimental topmost {*mpls-exp-value* | **qos-group** [**table** *table-map-name*]}

no set mpls experimental topmost {*mpls-exp-value* | **qos-group** [**table** *table-map-name*]}

Syntax Description

mpls-exp-value	Specifies the value used to set MPLS experimental bits defined by the policy map. Valid values are numbers from 0 to 7.
qos-group	Specifies that the **qos-group** packet-marking category is used to set the MPLS EXP imposition value. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category.
table	(Optional) Used in conjunction with the **qos-group** keyword. Indicates that the values set in a specified table map will be used to set the MPLS EXP value.
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the MPLS EXP value. The name can be a maximum of 64 alphanumeric characters.

Defaults

No MPLS EXP value is set.

Command Modes

QoS policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sets the MPLS EXP value only in the topmost label. This command does not affect an IP packet. The MPLS field in the topmost label header is not changed.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the qos-group packet-marking category to be used for mapping and setting the differentiated services code point (DSCP) value.

If you specify the qos-group category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the qos-group category as the MPLS EXP topmost value. For instance, if you configure the **set mpls experimental topmost qos-group** command, the QoS group value will be copied and used as the MPLS EXP topmost value.

The valid value range for the MPLS EXP topmost value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set mpls experimental topmost qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If a QoS group value exceeds the MPLS EXP topmost range (for example, 10), the packet-marking value will not copied and the packet will not be marked. No action is taken.

Examples

The following example shows how to set the MPLS EXP value to 3 in the topmost label of an input or output interface:

```
Router(config-pmap)# set mpls experimental topmost 3
```

The following example shows how to create the policy map named policy1 to use the packet-marking values defined in a table map named table-map1. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

The following example shows how to set the MPLS EXP value according to the QoS group value defined in table-map1.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set mpls experimental topmost qos-group table table-map1
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
match mpls experimental topmost	Matches the MPLS EXP field value in the topmost label.
set mpls experimental imposition	Sets the value of the MPLS EXP field on all imposed label entries.
set qos-group	Sets a group ID that can be used later to classify packets.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set mpls-label

To enable a route to be distributed with a Multiprotocol Label Switching (MPLS) label if the route matches the conditions specified in the route map, use the **set mpls-label** command in route-map configuration mode. To disable this function, use the **no** form of this command.

set mpls-label

no set mpls-label

Syntax Description

This command has no arguments or keywords.

Command Default

No route with an MPLS label is distributed.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command can be used only with the **neighbor route-map out** command to manage outbound route maps for a Border Gateway Protocol (BGP) session.

Use the **route-map** global configuration command with **match** and **set route-map** commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to create a route map that enables the route to be distributed with a label if the IP address of the route matches an IP address in ACL1:

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 1
```

```
Router(config-route-map)# set mpls-label
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or specifies an IPv6 access list to use to match packets for PBR for IPv6.
match mpls-label	Redistributes routes that contain MPLS labels and match the conditions specified in the route map.
neighbor route-map out	Manage outbound route maps for a BGP session.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set ospf router-id

To set a separate Open Shortest Path First (OSPF) router ID for each interface or subinterface on a provider edge (PE) router for each directly attached customer edge (CE) router, use the **set ospf router-id** command in route map configuration mode.

set ospf router-id

Syntax Description

This command has no arguments or keywords.

Defaults

OSPF router ID is not set.

Command Modes

Route map configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To use this command, you must enable OSPF and create a routing process.

Examples

The following example shows how to match the PE router IP address 192.168.0.0 against the interface in access list 1 and set to the OSPF router ID:

```
router ospf 2 vrfvpn1-site1
 redistribute bgp 100 metric-type 1 subnets
 network 202.0.0.0 0.0.0.255 area 1

router bgp 100
 neighbor 172.19.89. 62 remote-as 100
 access-list 1 permit 192.168.0.0
 route-map vpn1-site1-map permit 10
 match ip address 1
 set ospf router-id
```

Related Commands

Command	Description
router ospf	Enables OSPF routing, which places the router in router configuration mode.

set vrf

To enable Virtual Private Network (VPN) routing and forwarding (VRF) instance selection within a route map for policy-based routing VRF selection, use the **set vrf** command in route-map configuration mode. To disable VRF selection within a route map, use the **no** form of this command.

set vrf *vrf-name*

no set vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to the VRF.

Command Default

VPN VRF instance selection is not enabled within a route map for policy-based routing VRF selection.

Command Modes

Route-map configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The "Usage Guidelines" changed.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **set vrf** route-map configuration command was introduced with the Multi-VRF Selection Using Policy-Based Routing feature to provide a PBR mechanism for VRF selection. This command enables VRF selection by policy routing packets through a route map. The route map is attached to the incoming interface. Match criteria is defined in an IP access list or in an IP prefix list. Match criteria can also be defined based on packet length with the **match length** route map command. The VRF must be defined before you configure this command, and the **ip policy route-map** interface configuration command must be configured to enable policy routing under the interface or subinterface. If the VRF is not defined or if policy routing is not enabled, an error message will be displayed on the console when you attempt to configure the **set vrf** command.

Note The **set vrf** and **set ip global next-hop** commands can be configured with the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** commands. But the **set vrf** and **set ip global next-hop** commands take precedence over the **set default interface**, **set interface, set ip default next-hop**, and **set ip next-hop** commands. No error message is displayed if you attempt to configure the **set vrf** command with any of these four **set** commands.

Examples

The following example shows a route-map sequence that selects and sets a VRF based on match criteria defined in three different access lists. (The access list configuration is not shown in this example.) If the route map falls through and a match does not occur, the packet will be dropped if the destination is local.

```
route-map PBR-VRF-Selection permit 10
match ip address 40
set vrf VRF1
!
route-map PBR-VRF-Selection permit 20
match ip address 50
set vrf VRF2
!
route-map PBR-VRF-Selection permit 30
match ip address 60
set vrf VRF3
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
debug ip policy	Displays IP policy routing packet activity.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ip vrf	Configures a VRF routing table.
ip vrf receive	Inserts the IP address of an interface as a connected route entry in a VRF routing table.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to forward packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

show acircuit checkpoint

To display checkpointing information for each attachment circuit (AC), use the **show acircuit checkpoint** command in privileged EXEC mode.

show acircuit checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used for interface-based attachment circuits. For Frame Relay and ATM circuits, use the following commands to show redundancy information:

- **debug atm ha-error**
- **debug atm ha-events**
- **debug atm ha-state**
- **debug atm l2transport**
- **debug frame-relay redundancy**

Examples

The following **show acircuit checkpoint** command displays information about the ACs that have been check-pointed. The output varies, depending on whether the command output is for the active or standby Route Processor (RP).

On the active RP, the command displays the following output:

```
Router# show acircuit checkpoint

AC HA Checkpoint info:
Last Bulk Sync: 1 ACs
 AC    IW    XC    Id  VCId   Switch    Segment  St  Chkpt
----  ----  ----  ---  ----  --------  --------  --  -----
HDLC  LIKE  ATOM    3   100      1000      1000   0    N
VLAN  LIKE  ATOM    2  1002      2001      2001   3    Y
```

On the standby RP, the command displays the following output::

```
Router# show acircuit checkpoint

AC HA Checkpoint info:
 AC    IW    XC    Id  VCId   Switch    Segment  St  F-SLP
----  ----  ----  ---  ----  --------  --------  --  -----
HDLC  LIKE  ATOM    3   100         0         0   0   001
VLAN  LIKE  ATOM    2  1002      2001      2001   2   000
```

Table 13 describes the significant fields shown in the display.

Table 13 show acircuit checkpoint Field Descriptions

Field	Description
Last Bulk Sync	The number of ACs that were sent to the backup RP during the last bulk synchronization between the active and backup RPs.
AC	The type of attachment circuit.
IW	The type of interworking, either like-to-like (AToM) or any-to-any (Interworking).
XC	The type of cross-connect. Only AToM ACs are checkpointed.
ID	This field varies, depending on the type of attachment circuit. For Ethernet VLANs, the ID is the VLAN ID. For PPP and High-Level Data Link Control (HDLC), the ID is the AC circuit ID.
VCID	The configured virtual circuit ID.
Switch	An ID used to correlate the control plane and data plane contexts for this virtual circuit (VC). This is an internal value that is not for customer use.
Segment	An ID used to correlate the control plane and data plane contexts for this VC. This is an internal value that is not for customer use.
St	The state of the attachment circuit. This is an internal value that is not for customer use.
Chkpt	Whether the information about the AC was checkpointed.
F-SLP	Flags that provide more information about the state of the AC circuit. These values are not for customer use.

Related Commands

Command	Description
show mpls l2transport vc	Displays AToM status information.
show mpls l2transport vc checkpoint	Displays the status of the checkpointing process for both the active and standby RPs.

show atm vc

To display all ATM permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) and traffic information, use the **show atm vc** command in privileged EXEC mode.

show atm vc [*vcd* | **interface** *interface-number*]

Syntax Description

vcd	(Optional) Specifies the virtual circuit descriptor (VCD) about which to display information.
interface *interface-number*	(Optional) Interface number or subinterface number of the PVC or SVC. Displays all PVCs and SVCs on the specified interface or subinterface. The *interface-number* uses one of the following formats, depending on what router platform you are using: • For the ATM Interface Processor (AIP) on Cisco 7500 series routers; for the ATM port adapter, ATM-CES port adapter, and enhanced ATM port adapter on Cisco 7200 series routers; for the 1-port ATM-25 network module on Cisco 2600 and 3600 series routers: *slot*/**0**[**.***subinterface-number* **multipoint**] • For the ATM port adapter and enhanced ATM port adapter on Cisco 7500 series routers: *slot*/*port-adapter*/**0**[**.***subinterface-number* **multipoint**] • For the network processing module (NPM) on Cisco 4500 and Cisco 4700 routers: *number*[**.***subinterface-number* **multipoint**] For a description of these arguments, refer to the **interface atm** command.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.1CA	Information about VCs on an ATM-CES port adapter was added to the command output.
12.0(5)T	Information about VCs on an extended Multiprotocol Label Switching (MPLS) ATM interface was added to the command output.
12.2(25)S	Information about packet drops and errors was added to the command output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If no value is specified for the *vcd* argument, the command displays information for all PVCs and SVCs. The output is in summary form (one line per virtual circuit).

VCs on the extended MPLS ATM interfaces do not appear in the **show atm vc** command output. Instead, the **show xtagatm vc** command provides a similar output that shows information only on extended MPLS ATM VCs.

Examples

The following is sample output from the **show atm vc** command when no *vcd* value is specified. The status field is either ACTIVE or INACTIVE.

```
Router# show atm vc

Interface     VCD   VPI   VCI Type  AAL/Encaps     Peak   Avg.  Burst Status
ATM2/0          1     0     5  PVC  AAL5-SAAL     155000 155000    93 ACTIVE
ATM2/0.4        3     0    32  SVC  AAL5-SNAP     155000 155000    93 ACTIVE
ATM2/0.65432   10    10    10  PVC  AAL5-SNAP     100000  40000    10 ACTIVE
ATM2/0         99     0    16  PVC  AAL5-ILMI     155000 155000    93 ACTIVE
ATM2/0.105    250    33    44  PVC  AAL5-SNAP     155000 155000    93 ACTIVE
ATM2/0.100    300    22    33  PVC  AAL5-SNAP     155000 155000    93 ACTIVE
ATM2/0.12345 2047   255 65535  PVC  AAL5-SNAP         56     28  2047 ACTIVE
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified for a circuit emulation service (CES) circuit:

```
Router# show atm vc 2

ATM6/0: VCD: 2, VPI: 10, VCI: 10
PeakRate: 2310, Average Rate: 2310, Burst Cells: 94
CES-AAL1, etype:0x0, Flags: 0x20138, VCmode: 0x0
OAM DISABLED
InARP DISABLED
OAM cells received: 0
OAM cells sent: 334272
Status: ACTIVE
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, displaying statistics for that virtual circuit only:

```
Router# show atm vc 8

ATM4/0: VCD: 8, VPI: 8, VCI: 8
PeakRate: 155000, Average Rate: 155000, Burst Cells: 0
AAL5-LLC/SNAP, etype:0x0, Flags: 0x30, VCmode: 0xE000
OAM frequency: 0 second(s)
InARP frequency: 1 minute(s)
InPkts: 181061, OutPkts: 570499, InBytes: 757314267, OutBytes: 2137187609
InPRoc: 181011, OutPRoc: 10, Broadcasts: 570459
InFast: 39, OutFast: 36, InAS: 11, OutAS: 6
OAM cells received: 0
OAM cells sent: 0
Status: UP
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, AAL3/4 is enabled, an ATM Switched Multimegabit Data Service (SMDS) subinterface has been defined, and a range of message identifier numbers (MIDs) has been assigned to the PVC:

```
Router# show atm vc 1

ATM4/0.1: VCD: 1, VPI: 0, VCI: 1
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL3/4-SMDS, etype:0x1, Flags: 0x35, VCmode: 0xE200
MID start: 1, MID end: 16
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
```

```
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified and generation of Operation, Administration, and Maintenance (OAM) F5 loopback cells has been enabled:

```
Router# show atm vc 7

ATM4/0: VCD: 7, VPI: 7, VCI: 7
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL5-LLC/SNAP, etype:0x0, Flags: 0x30, VCmode: 0xE000
OAM frequency: 10 second(s)
InARP DISABLED
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast:0, OutFast:0, InAS:0, OutAS:0
OAM cells received: 0
OAM cells sent: 1
Status: UP
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, and there is an incoming multipoint virtual circuit:

```
Router# show atm vc 3

ATM2/0: VCD: 3, VPI: 0, VCI: 33
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL5-MUX, etype:0x809B, Flags: 0x53, VCmode: 0xE000
OAM DISABLED
InARP DISABLED
InPkts: 6646, OutPkts: 0, InBytes: 153078, OutBytes: 0
InPRoc: 6646, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
interface =  ATM2/0, call remotely initiated, call reference = 18082
vcnum = 3, vpi = 0, vci = 33, state = Active
 aal5mux vc, multipoint call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = never
Root Atm Nsap address: DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified, and there is an outgoing multipoint virtual circuit:

```
Router# show atm vc 6

ATM2/0: VCD: 6, VPI: 0, VCI: 35
PeakRate: 0, Average Rate: 0, Burst Cells: 0
AAL5-MUX, etype:0x800, Flags: 0x53, VCmode: 0xE000
OAM DISABLED
InARP DISABLED
InPkts: 0, OutPkts: 818, InBytes: 0, OutBytes: 37628
InPRoc: 0, OutPRoc: 0, Broadcasts: 818
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
interface =  ATM2/0, call locally initiated, call reference = 3
vcnum = 6, vpi = 0, vci = 35, state = Active
 aal5mux vc, multipoint call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = never
Leaf Atm Nsap address: DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
Leaf Atm Nsap address: CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12
```

The following is sample output from the **show atm vc** command when a *vcd* value is specified and there is a PPP-over-ATM connection:

```
Router# show atm vc 1

ATM8/0.1: VCD: 1, VPI: 41, VCI: 41
PeakRate: 155000, Average Rate: 155000, Burst Cells: 96
AAL5-CISCOPPP, etype:0x9, Flags: 0xC38, VCmode: 0xE000
virtual-access: 1, virtual-template: 1
OAM DISABLED
InARP DISABLED
InPkts: 13, OutPkts: 10, InBytes: 198, OutBytes: 156
InPRoc: 13, OutPRoc: 10, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM cells received: 0
OAM cells sent: 0
```

The following is sample output from the **show atm vc** command for IP multicast virtual circuits. The display shows the leaf count for multipoint VCs opened by the root. VCD 3 is a root of a multipoint VC with three leaf routers. VCD 4 is a leaf of some other router's multipoint VC. VCD 12 is a root of a multipoint VC with only one leaf router.

```
Router# show atm vc

            VCD/                                    Peak     Avg/Min     Burst
Interface   Name  VPI   VCI   Type     Encaps        Kbps     Kbps       Cells         Sts
0/0         1       0     5    PVC      SAAL       155000   155000       96          UP
0/0         2       0    16    PVC      ILMI       155000   155000       96          UP
0/0         3       0   124 MSVC-3      SNAP       155000   155000       96          UP
0/0         4       0   125   MSVC      SNAP       155000   155000       96          UP
0/0         5       0   126   MSVC      SNAP       155000   155000       96          UP
0/0         6       0   127   MSVC      SNAP       155000   155000       96          UP
0/0         9       0   130   MSVC      SNAP       155000   155000       96          UP
0/0         10      0   131    SVC      SNAP       155000   155000       96          UP
0/0         11      0   132 MSVC-3      SNAP       155000   155000       96          UP
0/0         12      0   133 MSVC-1      SNAP       155000   155000       96          UP
0/0         13      0   134    SVC      SNAP       155000   155000       96          UP
0/0         14      0   135 MSVC-2      SNAP       155000   155000       96          UP
0/0         15      0   136 MSVC-2      SNAP       155000   155000       96          UP
```

The following is sample output from the **show atm vc** command for an IP multicast virtual circuit. The display shows the owner of the VC and leaves of the multipoint VC. This VC was opened by IP multicast. The three leaf routers' ATM addresses are included in the display. The VC is associated with IP group address 10.1.1.1.

```
Router# show atm vc 11

ATM0/0: VCD: 11, VPI: 0, VCI: 132
PeakRate: 155000, Average Rate: 155000, Burst Cells: 96
AAL5-LLC/SNAP, etype:0x0, Flags: 0x650, VCmode: 0xE000
OAM DISABLED
InARP DISABLED
InPkts: 0, OutPkts: 12, InBytes: 0, OutBytes: 496
InPRoc: 0, OutPRoc: 0, Broadcasts: 12
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM cells received: 0
OAM cells sent: 0
Status: ACTIVE, TTL: 2, VC owner: IP Multicast (10.1.1.1)
interface =  ATM0/0, call locally initiated, call reference = 2
vcnum = 11, vpi = 0, vci = 132, state = Active
 aal5snap vc, multipoint call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = 00:00:00
```

```
Leaf Atm Nsap address: 47.0091810000000002BA08E101.444444444444.02
Leaf Atm Nsap address: 47.0091810000000002BA08E101.333333333333.02
Leaf Atm Nsap address: 47.0091810000000002BA08E101.222222222222.02
```

The following is sample output from the **show atm vc** command where no VCD is specified and private VCs are present:

```
Router# show atm vc

AAL /         Peak   Avg.  Burst
Interface     VCD   VPI   VCI Type  Encapsulation  Kbps   Kbps  Cells Status
ATM1/0          1     0    40  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          2     0    41  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          3     0    42  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          4     0    43  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0          5     0    44  PVC  AAL5-SNAP          0      0     0 ACTIVE
ATM1/0         15     1    32  PVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         17     1    34  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         26     1    43  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         28     1    45  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         29     1    46  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0         33     1    50  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
```

When you specify a VCD value and the VCD corresponds to that of a private VC on a control interface, the display output appears as follows:

```
Router# show atm vc 15

ATM1/0 33     1    50  TVC  AAL5-XTAGATM       0      0     0 ACTIVE
ATM1/0: VCD: 15, VPI: 1, VCI: 32, etype:0x8, AAL5 - XTAGATM, Flags: 0xD38
PeakRate: 0, Average Rate: 0, Burst Cells: 0, VCmode: 0x0
XTagATM1, VCD: 1, VPI: 0, VCI: 32
OAM DISABLED, InARP DISABLED
InPkts: 38811, OutPkts: 38813, InBytes: 2911240, OutBytes: 2968834
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM F5 cells sent: 0, OAM cells received: 0
Status: ACTIVE
```

Table 14 describes the fields shown in the displays.

Table 14 show atm vc Field Descriptions

Field	Description
Interface	Interface slot and port.
VCD/Name	Virtual circuit descriptor (virtual circuit number). The connection name is displayed if the virtual circuit (VC) was configured using the **pvc** command and the name was specified.
VPI	Virtual path identifier.
VCI	Virtual channel identifier.

Table 14 show atm vc Field Descriptions (continued)

Field	Description
Type	Type of VC, either PVC, SVC, TVC, or multipoint SVC (MSVC). • MSVC (with no -*x*) indicates that VCD is a leaf of some other router's multipoint VC. • MSVC-*x* indicates there are *x* leaf routers for that multipoint VC opened by the root. Type of PVC detected from PVC discovery, either PVC-D, PVC-L, or PVC-M. • PVC-D indicates a PVC created due to PVC discovery. • PVC-L indicates that the corresponding peer of this PVC could not be found on the switch. • PVC-M indicates that some or all of the quality of service (QoS) parameters of this PVC do not match those of the corresponding peer on the switch. • TVC indicates a Tag VC.
Encaps	Type of ATM adaptation layer (AAL) and encapsulation.
PeakRate	Kilobits per second sent at the peak rate.
Average Rate	Kilobits per second sent at the average rate.
Burst Cells	Value that equals the maximum number of ATM cells the VC can send at peak rate.
Status	Status of the VC connection. • UP indicates that the connection is enabled for data traffic. • DOWN indicates that the connection is not ready for data traffic. When the Status field is DOWN, a State field is shown. • INACTIVE indicates that the interface is down. • ACTIVE indicates that the interface is in use and active.
etype	Encapsulation type.

Table 14 show atm vc Field Descriptions (continued)

Field	Description
Flags	Bit mask describing VC information. The flag values are summed to result in the displayed value. 0x10000 ABR VC 0x20000 CES VC 0x40000 TVC 0x100 TEMP (automatically created) 0x200 MULTIPOINT 0x400 DEFAULT_RATE 0x800 DEFAULT_BURST 0x10 ACTIVE 0x20 PVC 0x40 SVC 0x0 AAL5-SNAP 0x1 AAL5-NLPID 0x2 AAL5-FRNLPID 0x3 AAL5-MUX 0x4 AAL3/4-SMDS 0x5 QSAAL 0x6 AAL5-ILMI 0x7 AAL5-LANE 0x8 AAL5-XTAGATM 0x9 CES-AAL1 0xA F4-OAM
VCmode	AIP-specific or NPM-specific register describing the usage of the VC. This register contains values such as rate queue, peak rate, and AAL mode, which are also displayed in other fields.
OAM frequency	Seconds between OAM loopback messages, or DISABLED if OAM is not in use on this VC.
InARP frequency	Minutes between Inverse Address Resolution Protocol (InARP) messages, or DISABLED if InARP is not in use on this VC.
virtual-access	Virtual access interface identifier.
virtual-template	Virtual template identifier.
InPkts	Total number of packets received on this VC. This number includes all fast-switched and process-switched packets.
OutPkts	Total number of packets sent on this VC. This number includes all fast-switched and process-switched packets.
InBytes	Total number of bytes received on this VC. This number includes all fast-switched and process-switched packets.
OutBytes	Total number of bytes sent on this VC. This number includes all fast-switched and process-switched packets.
InPRoc	Number of process-switched input packets.
OutPRoc	Number of process-switched output packets.
Broadcasts	Number of process-switched broadcast packets.
InFast	Number of fast-switched input packets.

Table 14 show atm vc Field Descriptions (continued)

Field	Description
OutFast	Number of fast-switched output packets.
InAS	Number of autonomous-switched or silicon-switched input packets.
VC TxRingLimit	Transmit Ring Limit for this VC.
VC Rx Limit	Receive Ring Limit for this VC.
Transmit priority	ATM service class transmit priority for this VC.
InCells	Number of incoming cells on this VC.
OutCells	Number of outgoing cells on this VC.
InPktDrops	A nonzero value for the InPktDrops of a VC counter suggests that the ATM interface is running out of packet buffers for an individual VC, or is exceeding the total number of VC buffers that can be shared by the VCs.
OutPktDrops	The PA-A3 driver increments the OutPktDrops counter when a VC fills its individual transmit buffer quota. The purpose of the quota is to prevent a consistently oversubscribed VC from grabbing all of the packet buffer resources and hindering other VCs from transmitting normal traffic within their traffic contracts.
InCellDrops	Number of incoming cells dropped on this VC.
OutCellDrops	Number of outgoing cells dropped on this VC.
InByteDrops	Number of incoming bytes that are dropped on this VC.
OutByteDrops	Number of outgoing bytes that are dropped on this VC.
CrcErrors	Number of cyclic redundancy check (CRC) errors on this VC.
SarTimeOuts	Number of segmentation and reassembly sublayer time-outs on this VC.
OverSizedSDUs	Number of over-sized service data units on this VC
LengthViolation	Number of length violations on this VC. A length violation occurs when a reassembled packet is dropped without checking the CRC.
CPIErrors	The Common Part Indicator error field is a one octet field in the AAL5 encapsulation of an ATM cell and must be set to 0. If it is received with some other value, it is flagged as an error by the interface. For example, this error may indicate data corruption.
Out CLP	Number of packets or cells where the Output Cell Loss Priority bit is set.
OutAS	Number of autonomous-switched or silicon-switched output packets.
OAM cells received	Number of OAM cells received on this VC.
OAM cells sent	Number of OAM cells sent on this VC.
TTL	Time to live in ATM hops across the VC.
VC owner	IP Multicast address of the group.

Related Commands

Command	Description
atm nsap-address	Sets the NSAP address for an ATM interface using SVC mode.
show xtagatm vc	Displays information about the VCs on the extended MPLS ATM interfaces.

show connection

To display the status of interworking connections, use the **show connection** command in privileged EXEC mode.

show connection [**all** | *element* | **id** *ID* | **name** *name* | **port** *port*]

Syntax Description

all	(Optional) Displays information about all interworking connections.
element	(Optional) Displays information about the specified connection element.
id *ID*	(Optional) Displays information about the specified connection identifier.
name *name*	(Optional) Displays information about the specified connection name.
port *port*	(Optional) Displays information about all connections on an interface. (In Cisco IOS Release 12.0S, only ATM, serial, and Fast Ethernet are shown.)

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)T	This command was introduced as **show connect** (FR-ATM).
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S and updated to show all ATM, serial, and Fast Ethernet interworking connections.
12.4(2)T	The command output was modified to add Segment 1 and Segment 2 fields for Segment state and channel ID.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(8)	This command was integrated into Cisco IOS Release 12.4(8).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was updated to display High-Level Data Link Control (HDLC) local switching connections.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following example shows the local interworking connections on a router:

```
Router# show connection

ID   Name               Segment 1            Segment 2           State
=====================================================================
1    conn1          ATM 1/0/0 AAL5 0/100   ATM 2/0/0 AAL5 0/100   UP
```

```
2     conn2          ATM 2/0/0 AAL5 0/300   Serial0/1 16           UP
3     conn3          ATM 2/0/0 AAL5 0/400   FA 0/0.1 10            UP
4     conn4          ATM 1/0/0 CELL 0/500   ATM 2/0/0 CELL 0/500   UP
5     conn5          ATM 1/0/0 CELL 100     ATM 2/0/0 CELL 100     UP
```

Table 15 describes the significant fields shown in the display.

Table 15 show connection Field Descriptions

Field	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.
Segment 1 Segment 2	Information about the interworking segments: • Interface name and number. • Segment state, interface name and number, and channel ID. Segment state will displays nothing if the segment state is UP, "-" if the segment state is DOWN, and "***Card Removed***" if the segment state is DETACHED. • Type of encapsulation (if any) assigned to the interface. • Permanent virtual circuit (PVC) assigned to the ATM interface, data-link connection identifier (DLCI) assigned to the serial interface, or VLAN ID assigned to the Ethernet interface.
State	Status of the connection, which is one of the following: INVALID, UP, ADMIN UP, ADMIN DOWN, OPER DOWN, COMING UP, NOT VERIFIED, ERR.

Related Commands

Command	Description
connect (L2VPN local switching)	Connects two different or like interfaces on a router.
show atm pvc	Displays the status of ATM PVCs and SVCs.
show frame-relay pvc	Displays the status of Frame Relay interfaces.

show controllers vsi control-interface

Note Effective with Cisco IOS Release 12.4(20)T, the **show controller vsi control-interface** command is not available in Cisco IOS software.

To display information about an ATM interface configured with the **tag-control-protocol vsi** command to control an external switch (or if an interface is not specified, to display information about all Virtual Switch Interface [VSI] control interfaces), use the **show controllers vsi control-interface** command in user EXEC or privileged EXEC mode.

show controllers vsi control-interface [*interface*]

Syntax Description

interface	(Optional) Specifies the interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	Thsi command was removed.

Examples

The following is sample output from the **show controllers vsi control-interface** command:

```
Router# show controllers vsi control-interface

Interface:           ATM2/0       Connections:         14
```

The display shows the number of cross-connects currently on the switch that were established by the MPLS LSC through the VSI over the control interface.

Table 17 describes the significant fields shown in the display.

Table 16 show controllers vsi control-interface Field Descriptions

Field	Description
Interface	The (Cisco IOS) interface name.
Connections	The number of cross connections currently on the switch.

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi descriptor

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi descriptor** command is not available in Cisco IOS software.

To display information about a switch interface discovered by the Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC) through a Virtual Switch Interface (VSI), or if no descriptor is specified, about all such discovered interfaces, use the **show controllers vsi descriptor** command in user EXEC or privileged EXEC mode.

show controllers vsi descriptor [*descriptor*]

Syntax Description

descriptor	(Optional) Physical descriptor. For the Cisco BPX switch, the physical descriptor has the following form: *slot.port.0*

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

Specify an interface by its (switch-supplied) physical descriptor.

Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information is displayed when you enter the **show controllers xtagatm** privileged EXEC command. However, you must specify a Cisco IOS interface name instead of a physical descriptor.

Examples

The following is sample output from the **show controllers vsi descriptor** command:

```
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
```

Table 17 describes the significant fields shown in the display.

Table 17 show controllers vsi descriptor Field Descriptions

Field	Description
Phys desc	Physical descriptor. A string learned from the switch that identifies the interface.
Log intf	Logical interface ID. This 32-bit entity, learned from the switch, uniquely identifies the interface.
Interface	The (Cisco IOS) interface name.
IF status	Overall interface status. Can be “up,” “down,” or “administratively down.”
Min VPI	Minimum virtual path identifier. Indicates the low end of the VPI range configured on the switch.
Max VPI	Maximum virtual path identifier. Indicates the high end of the VPI range configured on the switch.
Min VCI	Minimum virtual path identifier. Indicates the high end of the VCI range configured on the switch.
Max VCI	Maximum virtual channel identifier. Indicates the high end of the VCI range configured on, or determined by, the switch.
IFC state	Operational state of the interface, according to the switch. Can be one of the following: • FAILED_EXT (that is, an external alarm) • FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
Maximum cell rate	Maximum cell rate for the interface, which has been configured on the switch (in cells per second).
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Available cell rate (forward)	Cell rate that is currently available in the forward (that is, ingress) direction for new cross-connects on the interface.
Available cell rate (backward)	Cell rate that is currently available in the backward (that is, egress) direction for new cross-connects on the interface.

Related Commands

Command	Description
show controllers xtagatm	Displays information about an extended MPLS ATM interface.

show controllers vsi session

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi session** command is not available in Cisco IOS software.

To display information about all sessions with Virtual Switch Interface (VSI) slaves, use the **show controllers vsi session** command in user EXEC or privileged EXEC mode.

show controllers vsi session [*session-number* [**interface** *interface*]]

Note 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 BPX, each port or trunk card assumes the role of a VSI slave.

Syntax Description

session-number	(Optional) Specifies the session number.
interface *interface*	(Optional) Specifies the VSI control interface.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

If a session number and an interface are specified, detailed information on the individual session is presented. If the session number is specified, but the interface is omitted, detailed information on all sessions with that number is presented. (Only one session can contain a given number, because multiple control interfaces are not supported.)

Examples

The following is sample output from the **show controllers vsi session** command:

```
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
```

Table 18 describes the significant fields shown in the display.

Table 18 show controllers vsi session Field Descriptions

Field	Description
Interface	Control interface name.
Session	Session number (from 0 to <*n*–1>), where *n* is the number of sessions on the control interface.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC carrying the VSI protocol between the master and the slave for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier (for the VC used for this session).
Switch/Slave Ids	Switch and slave identifiers supplied by the switch.
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. Other possible states include the following: • CONFIGURING • RESYNC-STARTING • RESYNC-UNDERWAY • RESYNC-ENDING • DISCOVERY • SHUTDOWN-STARTING • SHUTDOWN-ENDING • INACTIVE

In the following example, session number 9 is specified with the **show controllers vsi session** command:

```
Router# show controllers vsi session 9

Interface:            ATM1/0        Session number:       9
VCD:                  10            VPI/VCI:              0/49
Switch type:          BPX           Switch id:            0
Controller id:        1             Slave id:             10
Keepalive timer:      15            Powerup session id:   0x0000000A
Cfg/act retry timer:  8/8           Active session id:    0x0000000A
Max retries:          10            Ctrl port log intf:   0x000A0100
Trap window:          50            Max/actual cmd wndw:  21/21
Trap filter:          all           Max checksums:        19
Current VSI version:  1             Min/max VSI version:  1/1
Messages sent:        2502          Inter-slave timer:    4.000
Messages received:    2502          Messages outstanding: 0
```

Table 19 describes the significant fields shown in the display.

Table 19 show controllers vsi session Field Descriptions

Field	Description
Interface	Name of the control interface on which this session is configured.
Session number	A number from 0 to <*n*–1>, where *n* is the number of slaves. Configured on the MPLS LSC with the *slaves* option of the **tag-control-protocol vsi** command.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC that carries VSI protocol messages for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier for the VC used for this session.
Switch type	Switch device (for example, the BPX).
Switch id	Switch identifier (supplied by the switch).
Controller id	Controller identifier. Configured on the LSC, and on the switch, with the **id** option of the **tag-control-protocol vsi** command.
Slave id	Slave identifier (supplied by the switch).
Keepalive timer	VSI master keepalive timeout period (in seconds). Configured on the MPLS LSC through the **keepalive** option of the **tag-control-protocol-vsi** command. If no valid message is received by the MPLS LSC within this time period, it sends a keepalive message to the slave.
Powerup session id	Session ID (supplied by the slave) used at powerup time.
Cfg/act retry timer	Configured and actual message retry timeout period (in seconds). If no response is received for a command sent by the master within the actual retry timeout period, the message is re-sent. This applies to most message transmissions. The configured retry timeout value is specified through the **retry** option of the **tag-control-protocol vsi** command. The actual retry timeout value is the larger of the configured value and the minimum retry timeout value permitted by the switch.
Active session id	Session ID (supplied by the slave) for the currently active session.
Max retries	Maximum number of times that a particular command transmission will be retried by the master. That is, a message may be sent up to <max_retries+1> times. Configured on the MPLS LSC through the **retry** option of the **tag-control-protocol vsi** command.
Ctrl port log intf	Logical interface identifier for the control port, as supplied by the switch.
Trap window	Maximum number of outstanding trap messages permitted by the master. This is advertised, but not enforced, by the LSC.
Max/actual cmd wndw	Maximum command window is the maximum number of outstanding (that is, unacknowledged) commands that may be sent by the master before waiting for acknowledgments. This number is communicated to the master by the slave. The command window is the maximum number of outstanding commands that are permitted by the master, before it waits for acknowledgments. This is always less than the maximum command window.
Trap filter	This is always “all” for the LSC, indicating that it wants to receive all traps from the slave. This is communicated to the slave by the master.

Table 19 show controllers vsi session Field Descriptions

Field	Description
Max checksums	Maximum number of checksum blocks supported by the slave.
Current VSI version	VSI protocol version currently in use by the master for this session.
Min/max VSI version	Minimum and maximum VSI versions supported by the slave, as last reported by the slave. If both are zero, the slave has not yet responded to the master.
Messages sent	Number of commands sent to the slave.
Inter-slave timer	Timeout value associated by the slave for messages it sends to other slaves. On a VSI-controlled switch with a distributed slave implementation (such as the BPX), VSI messages may be sent between slaves to complete their processing. For the MPLS LSC VSI implementation to function properly, the value of its retry timer is forced to be at least two times the value of the interslave timer. (See "Cfg/act retry timer" in this table.)
Messages received	Number of responses and traps received by the master from the slave for this session.
Messages outstanding	Current number of outstanding messages (that is, commands sent by the master for which responses have not yet been received).

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi status

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi status** command is not available in Cisco IOS software.

To display a one-line summary of each Virtual Switch Interface (VSI)-controlled interface, use the **show controllers vsi status** command in user EXEC or privileged EXEC mode.

show controllers vsi status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

If an interface is discovered by the LSC, but no extended Multiprotocol Label Switching (MPLS) ATM interface is associated with it through the **extended-port** command, then the interface name is marked <unknown>, and interface status is marked n/a.

Examples

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
```

Table 20 describes the significant fields shown in the display.

Table 20 show controllers vsi status Field Descriptions

Field	Description
Interface Name	The (Cisco IOS) interface name.
IF Status	Overall interface status. Can be “up,” “down,” or “administratively down.”

Table 20 show controllers vsi status Field Descriptions (continued)

Field	Description
IFC State	The operational state of the interface, according to the switch. Can be one of the following: • FAILED-EXT (that is, an external alarm) • FAILED-INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
Physical Descriptor	A string learned from the switch that identifies the interface.

show controllers vsi traffic

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers vsi traffic** command is not available in Cisco IOS software.

To display traffic information about Virtual Switch Interface (VSI)-controlled interfaces, VSI sessions, or virtual circuits (VCs) on VSI-controlled interfaces, use the **show controllers vsi traffic** command in user EXEC or privileged EXEC mode.

show controllers vsi traffic {**descriptor** *descriptor* | **session** *session-number* | **vc** [**descriptor** *descriptor* [*vpi vci*]]}

Syntax Description

descriptor *descriptor*	Displays traffic statistics for the specified descriptor.
session *session-number*	Displays traffic statistics for the specified session.
vc	Displays traffic statistics for the specified VC.
descriptor [**descriptor** *descriptor*]	Specifies the name of the physical descriptor.
vpi	Virtual path identifier (0 to 4095).
vci	Virtual circuit identifier (0 to 65535).

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	The VPI range of values was extended to 4095.
12.4(20)T	This command was removed.

Usage Guidelines

If none of the keywords is specified, traffic for all interfaces is displayed. You can specify a single interface by its (switch-supplied) physical descriptor. For the BPX switch, the physical descriptor has the form

slot.port. 0

If a session number is specified, the output displays VSI protocol traffic by message type. The VC traffic display is also displayed by the **show xmplsatm vc cross-connect traffic descriptor** command.

Examples

The following is sample output from the **show controllers vsi traffic** command:

```
Router# show controllers vsi traffic

Phys desc: 10.1.0
Interface: switch control port
```

```
IF status: n/a
Rx cells: 304250            Rx cells discarded: 0
Tx cells: 361186            Tx cells discarded: 0
Rx header errors: 4294967254 Rx invalid addresses (per card): 80360
Last invalid address: 0/53

Phys desc: 10.2.0
Interface: XTagATM0
IF status: up
Rx cells: 202637            Rx cells discarded: 0
Tx cells: 194979            Tx cells discarded: 0
Rx header errors: 4294967258 Rx invalid addresses (per card): 80385
Last invalid address: 0/32

Phys desc: 10.3.0
Interface: XTagATM1
IF status: up
Rx cells: 182295            Rx cells discarded: 0
Tx cells: 136369            Tx cells discarded: 0
Rx header errors: 4294967262 Rx invalid addresses (per card): 80372
Last invalid address: 0/32
```

Table 21 describes the significant fields shown in the display.

Table 21 show controllers vsi traffic Field Descriptions

Field	Description
Phys desc	Physical descriptor of the interface.
Interface	The Cisco (IOS) interface name.
Rx cells	Number of cells received on the interface.
Tx cells	Number of cells transmitted on the interface.
Rx cells discarded	Number of cells received on the interface that were discarded due to traffic management.
Tx cells discarded	Number of cells that could not be transmitted on the interface due to traffic management and which were therefore discarded.
Rx header errors	Number of cells that were discarded due to ATM header errors.
Rx invalid addresses	Number of cells received with an invalid address (that is, an unexpected VPI/VCI combination). With the Cisco BPX switch, this count is of all such cells received on all interfaces in the port group of this interface.
Last invalid address	Number of cells received on this interface with ATM cell header errors.

The following sample output is displayed when you enter the **show controllers vsi traffic session 9** command:

```
Router# show controllers vsi traffic session 9
                        Sent                                Received
Sw Get Cnfg Cmd:         3656       Sw Get Cnfg Rsp:         3656
Sw Cnfg Trap Rsp:        0          Sw Cnfg Trap:            0
Sw Set Cnfg Cmd:         1          Sw Set Cnfg Rsp:         1
Sw Start Resync Cmd:     1          Sw Start Resync Rsp:     1
Sw End Resync Cmd:       1          Sw End Resync Rsp:       1
Ifc Getmore Cnfg Cmd:    1          Ifc Getmore Cnfg Rsp:    1
Ifc Cnfg Trap Rsp:       4          Ifc Cnfg Trap:           4
Ifc Get Stats Cmd:       8          Ifc Get Stats Rsp:       8
Conn Cmt Cmd:            73         Conn Cmt Rsp:            73
```

```
Conn Del Cmd:            50         Conn Del Rsp:            0
Conn Get Stats Cmd:      0          Conn Get Stats Rsp:      0
Conn Cnfg Trap Rsp:      0          Conn Cnfg Trap:          0
Conn Bulk Clr Stats Cmd: 0          Conn Bulk Clr Stats Rsp: 0
Gen Err Rsp:             0          Gen Err Rsp:             0
unused:                  0          unused:                  0
unknown:                 0          unknown:                 0
TOTAL:                   3795       TOTAL:                   3795
```

Table 22 describes the significant fields shown in the display.

Table 22 show controllers vsi traffic session Field Descriptions

Field	Description
Sw Get Cnfg Cmd	Number of VSI “get switch configuration command” messages sent.
Sw Cnfg Trap Rsp	Number of VSI “switch configuration asynchronous trap response” messages sent.
Sw Set Cnfg Cmd	Number of VSI “set switch configuration command” messages sent.
Sw Start Resync Cmd	Number of VSI “set resynchronization start command” messages sent.
Sw End Resync Cmd	Number of VSI “set resynchronization end command” messages sent.
Ifc Getmore Cnfg Cmd	Number of VSI “get more interfaces configuration command” messages sent.
Ifc Cnfg Trap Rsp	Number of VSI “interface configuration asynchronous trap response” messages sent.
Ifc Get Stats Cmd	Number of VSI “get interface statistics command” messages sent.
Conn Cmt Cmd	Number of VSI “set connection committed command” messages sent.
Conn Del Cmd	Number of VSI “delete connection command” messages sent.
Conn Get Stats Cmd	Number of VSI “get connection statistics command” messages sent.
Conn Cnfg Trap Rsp	Number of VSI “connection configuration asynchronous trap response” messages sent.
Conn Bulk Clr Stats Cmd	Number of VSI “bulk clear connection statistics command” messages sent.
Gen Err Rsp	Number of VSI “generic error response” messages sent or received.
Sw Get Cnfg Rsp	Number of VSI “get connection configuration command response” messages received.
Sw Cnfg Trap	Number of VSI “switch configuration asynchronous trap” messages received.
Sw Set Cnfg Rsp	Number of VSI “set switch configuration response” messages received.
Sw Start Resync Rsp	Number of VSI “set resynchronization start response” messages received.
Sw End Resync Rsp	Number of VSI “set resynchronization end response” messages received.
Ifc Getmore Cnfg Rsp	Number of VSI “get more interfaces configuration response” messages received.
Ifc Cnfg Trap	Number of VSI “interface configuration asynchronous trap” messages received.
Ifc Get Stats Rsp	Number of VSI “get interface statistics response” messages received.
Conn Cmt Rsp	Number of VSI “set connection committed response” messages received.

Table 22 show controllers vsi traffic session Field Descriptions (continued)

Field	Description
Conn Del Rsp	Number of VSI “delete connection response” messages received.
Conn Get Stats Rsp	Number of VSI “get connection statistics response” messages received.
Conn Cnfg Trap	Number of VSI “connection configuration asynchronous trap” messages received.
Conn Bulk Clr Stats Rsp	Number of VSI “bulk clear connection statistics response” messages received.
unused, unknown	“Unused” messages are those whose function codes are recognized as being part of the VSI protocol, but which are not used by the MPLS LSC and, consequently, are not expected to be received or sent. “Unknown” messages have function codes that the MPLS LSC does not recognize as part of the VSI protocol.
TOTAL	Total number of VSI messages sent or received.

show controllers xtagatm

Note Effective with Cisco IOS Release 12.4(20)T, the **show controllers xtagatm** command is not available in Cisco IOS software.

To display information about an extended Multiprotocol Label Switching (MPLS) ATM interface controlled through the Virtual Switch Interface (VSI) protocol (or, if an interface is not specified, to display information about all extended MPLS ATM interfaces controlled through the VSI protocol), use the **show controllers xtagatm** command in user EXEC or privileged EXEC mode.

show controllers xtagatm *if-number*

Syntax Description

if-number	Specifies the interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

Per-interface information includes the following:

- Interface name
- Physical descriptor
- Interface status
- Physical interface state (supplied by the switch)
- Acceptable VPI and VCI ranges
- Maximum cell rate
- Available cell rate (forward/backward)
- Available channels

Similar information appears if you enter the **show controllers vsi descriptor** command. However, you must specify an interface by its (switch-supplied) physical descriptor, instead of its Cisco IOS interface name. For the Cisco BPX switch, the physical descriptor has the form *slot.port.0*.

Examples

In this example, the sample output is from the **show controllers xtagatm** command specifying interface 0:

```
Router# show controllers xtagatm 0
```

```
Interface XTagATM0 is up
Hardware is Tag-Controlled ATM Port (on BPX switch BPX-VSI1)
Control interface ATM1/0 is up
Physical descriptor is 10.2.0
Logical interface 0x000A0200 (0.10.2.0)
Oper state ACTIVE, admin state UP
VPI range 1-255, VCI range 32-65535
VPI is not translated at end of link
Tag control VC need not be strictly in VPI/VCI range
Available channels: ingress 30, egress 30
Maximum cell rate: ingress 300000, egress 300000
Available cell rate: ingress 300000, egress 300000
Endpoints in use: ingress 7, egress 8, ingress/egress 1
Rx cells 134747
rx cells discarded 0, rx header errors 0
rx invalid addresses (per card): 52994
last invalid address 0/32
Tx cells 132564
tx cells discarded: 0
```

Table 23 describes the significant fields shown in the display.

Table 23 show controllers xtagatm Field Descriptions

Field	Description
Interface XTagATM0 is up	Indicates the overall status of the interface. May be “up,” “down,” or “administratively down.”
Hardware is Tag-Controlled ATM Port	Indicates the hardware type. If the XTagATM was successfully associated with a switch port, a description of the form (on <switch_type> switch <name>) follows this field, where <switch_type> indicates the type of switch (for example, BPX), and the name is an identifying string learned from the switch. If the XTagATM interface was not bound to a switch interface (with the **extended-port** interface configuration command), then the label “Not bound to a control interface and switch port” appears. If the interface has been bound, but the target switch interface has not been discovered by the LSC, then the label “Bound to undiscovered switch port (id <number>)” appears, where <number> is the logical interface ID in hexadecimal notation.
Control interface ATM1/0 is up	Indicates that the XTagATM interface was bound (with the **extended-port** interface configuration command) to the VSI master whose control interface is ATM1/0 and that this control interface is up.
Physical descriptor is...	A string identifying the interface that was learned from the switch.
Logical interface	This 32-bit entity, learned from the switch, uniquely identifies the interface. It appears in both hexadecimal and dotted quad notation.

Table 23 show controllers xtagatm Field Descriptions (continued)

Field	Description
Oper state	Operational state of the interface, according to the switch. Can be one of the following: • ACTIVE • FAILED_EXT (that is, an external alarm) • FAILED_INT (indicates the inability of the MPLS LSC to communicate with the VSI slave controlling the interface, or another internal failure) • REMOVED (administratively removed from the switch)
admin state	Administrative state of the interface, according to the switch—either "Up" or "Down."
VPI range 1 to 255	Indicates the allowable VPI range for the interface that was configured on the switch.
VCI range 32 to 65535	Indicates the allowable VCI range for the interface that was configured on, or determined by, the switch.
LSC control VC need not be strictly in VPI or VCI range	Indicates that the label control VC does not need to be within the range specified by VPI range, but may be on VPI 0 instead.
Available channels	Indicates the number of channels (endpoints) that are currently free to be used for cross-connects.
Maximum cell rate	Maximum cell rate for the interface, which was configured on the switch.
Available cell rate	Cell rate that is currently available for new cross-connects on the interface.
Endpoints in use	Number of endpoints (channels) in use on the interface, broken down by anticipated traffic flow, as follows: • Ingress—Endpoints carry traffic into the switch • Egress—Endpoints carry traffic away from the switch • Ingress/egress—Endpoints carry traffic in both directions
Rx cells	Number of cells received on the interface.
rx cells discarded	Number of cells received on the interface that were discarded due to traffic management actions (rx header errors).
rx header errors	Number of cells received on the interface with cell header errors.
rx invalid addresses (per card)	Number of cells received with invalid addresses (that is, unexpected VPI or VCI.). On the BPX, this counter is maintained per port group (not per interface).
last invalid address	Address of the last cell received on the interface with an invalid address (for example, 0/32).
Tx cells	Number of cells sent from the interface.
tx cells discarded	Number of cells intended for transmission from the interface that were discarded due to traffic management actions.

Related Commands

Command	Description
show controllers vsi descriptor	Displays information about a switch interface discovered by the MPLS LSC through the VSI.

show interface tunnel configuration

To display the configuration of a mesh tunnel interface, use the **show interface tunnel configuration** command in privileged EXEC mode.

show interface tunnel *num* **configuration**

Syntax Description

num	Number of the mesh tunnel for which you want to display configuration information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The space before the *num* argument is optional.

Use this command to show the running configuration of the mesh tunnel interface.

Examples

The following command output shows the configuration of mesh tunnel interface 5:

```
Router# show interface tunnel 5 configuration

interface tunnel 5
 ip unnumbered Loopback0
 no ip directed-broadcast
 no keepalive
 tunnel destination access-list 1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
```

Table 24 describes the significant fields shown in the display.

Table 24 show interface tunnel configuration Field Descriptions

Field	Description
ip unnumbered Loopback0	Indicates the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.
no ip directed-broadcast	Indicates that no IP broadcast addresses are used for the mesh tunnel interface.

Table 24 show interface tunnel configuration Field Descriptions (continued)

Field	Description
no keepalive	Indicates that no keepalives are set for the mesh tunnel interface.
tunnel destination access-list 1	Indicates that access-list 1 is the access list that the template interface will use for obtaining the mesh tunnel interface destination address.
tunnel mode mpls traffic-eng	Indicates that the mode of the mesh tunnel is set to Multiprotocol Label Switching (MPLS) for traffic engineering.
tunnel mpls traffic-eng autoroute announce	Indicates that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.
tunnel mpls traffic-eng path-option 1 dynamic	Indicates that a path option (path-option1) for the label switch router (LSR) for the MPLS traffic engineering (TE) mesh tunnel is configured dynamically.

Related Commands

Command	Description
tunnel destination access-list	Specifies the access list that the template interface will use for obtaining the mesh tunnel interface destination address.

show interface xtagatm

Note Effective with Cisco IOS Release 12.4(20)T, the **show interface xtagatm** command is not available in Cisco IOS software.

To display information about an extended Multiprotocol Label Switching (MPLS) ATM interface, use the **show interface xtagatm** command in user EXEC or privileged EXEC mode.

show interface xtagatm *if-number*

Syntax Description

if-number	Specifies the MPLS ATM interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3T	Sample command output was added for when an interface is down.
12.4(20)T	This command was removed.

Usage Guidelines

Extended MPLS ATM interfaces are virtual interfaces that are created on first reference like tunnel interfaces. Extended MPLS ATM interfaces are similar to ATM interfaces except that the former only supports LC-ATM encapsulation.

Examples

The following is sample command output when an interface is down:

```
Router# show interface xt92

XTagATM92 is down, line protocol is down
 Hardware is Tag-Controlled Switch Port
 Interface is unnumbered. Using address of Loopback1 (15.15.15.15)
 MTU 4470 bytes, BW 4240 Kbit, DLY 80 used,
 reliability 186/255, txload 1/255, rxload 1/255
 Encapsulation ATM, loopback not set
 Keepalive set (10 sec) [00:00:08/4]
 Encapsulation(s): AAL5
 Control interface: not configured
 0 terminating VCs
 Switch port traffic:
  ? cells input, ? cells output
 Last input 00:00:10, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/0 (size/max)
 Terminating traffic:
```

```
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
  138 packets input, 9193 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 i
  00:05:46: %SYS-5-CONFIG_I: Configured from console by consolegnored, 0 abort
  142 packets output, 19686 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
```

The following is sample command output when an interface is up:

```
Router# show interface xt92
XTagATM92 is up, line protocol is up
Hardware is Tag-Controlled Switch Port
Interface is unnumbered. Using address of Loopback1 (15.15.15.15)
MTU 4470 bytes, BW 4240 Kbit, DLY 80 used,
reliability 174/255, txload 1/255, rxload 1/255
Encapsulation ATM, loopback not set
Keepalive set (10 sec)
Encapsulation(s): AAL5
Control interface: ATM3/0, switch port: bpx 9.2
3 terminating VCs, 7 switch cross-connects
Switch port traffic:
275 cells input, 273 cells output
Last input 00:00:00, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
Terminating traffic:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
127 packets input, 8537 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
131 packets output, 18350 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

Table 25 describes the significant fields shown in the displays.

Table 25 show interface xtagatm Field Descriptions

Field	Description
XTagATM0 is up XTagATM0 is down	Interface is currently active (up) or inactive (down).
line protocol is up line protocol is down	Displays the line protocol as up or down.
Hardware is Tag-Controlled Switch Port	Specifies the hardware type.
Interface is unnumbered	Specifies that this is an unnumbered interface.
MTU	Maximum transmission unit of the extended MPLS ATM interface.
BW	Bandwidth of the interface (in kBps).
DLY	Delay of the interface in microseconds.

Table 25 show interface xtagatm Field Descriptions

Field	Description
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
Encapsulation ATM	Encapsulation method.
loopback not set	Indicates that loopback is not set.
Keepalive set (10 sec) [00:00:08/4]	Indicates why the Xtag line is down. Valid values are: 1—Internal usage. 2—Administratively down. 3—Internal usage. 4—No extended port is configured. 5—Some cross-connects from an old session have been left operational. 6—No extended port or a wrong extended port was configured. 7—No control port was configured. 8—Internal usage. 9—Internal usage. 10—Internal usage. 11—Internal usage. 12—External port. The XTag is mapped to an invalid port on the switch. 13—External port. The XTag is mapped to a port that is down. 14—External port is mapped to the control panel on the switch. 15—OAM is being used to track the link state. The neighbor may be down or it is not responding to the OAM calls.
Encapsulation(s)	Identifies the ATM adaptation layer.
Control interface	Identifies the control port switch port with which the extended MPLS ATM interface has been associated through the **extended-port** interface configuration command.
n terminating VCs	Number of terminating VCs with an endpoint on this extended MPLS ATM interface. Packets are sent or received by the MPLS LSC on a terminating VC, or are forwarded between an LSC-controlled switch port and a router interface.
7 switch cross-connects	Number of switch cross-connects on the external switch with an endpoint on the switch port that corresponds to this interface. This includes cross-connects to terminating VCs that carry data to and from the LSC, and cross-connects that bypass the MPLS LSC and switch cells directly to other ports.
Switch port traffic	Number of cells received and sent on all cross-connects associated with this interface.
Terminating traffic	Indicates that counters below this line apply only to packets sent or received on terminating VCs.

Table 25 show interface xtagatm Field Descriptions

Field	Description
5-minute input rate, 5-minute output rate	Average number of bits and packets sent per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet systems and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored and abort counts. Other input-related errors can also increment the count, so that this sum may not balance with other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of traffic collisions or a station sending bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface. This usually indicates a clocking problem between the interface and the data-link equipment.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times that the sender has been running faster than the router can handle data. This condition may never be reported on some interfaces.

Table 25 show interface xtagatm Field Descriptions

Field	Description
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages re-sent due to an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only one time in output packets.
interface resets	Number of times an interface has been completely reset. Resets occur if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

Related Commands

Command	Description
interface xtagatm	Enters configuration mode for an extended MPLS ATM (XTagATM) interface.

show ip bgp labels

To display information about Multiprotocol Label Switching (MPLS) labels from the external Border Gateway Protocol (eBGP) route table, use the **show ip bgp labels** command in privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to display eBGP labels associated with an Autonomous System Boundary Router (ASBR).

This command displays labels for BGP routes in the default table only. To display labels in the Virtual Private Network (VPN) routing and forwarding (VRF) tables, use the **show ip bgp vpnv4** {**all | vrf** *vrf-name*} command with the optional **labels** keyword.

Examples

The following example shows output for an ASBR using BGP as a label distribution protocol:

```
Router# show ip bgp labels

Network          Next Hop         In Label/Out Label
10.3.0.0/16       0.0.0.0          imp-null/exp-null
10.15.15.15/32   10.15.15.15      18/exp-null
10.16.16.16/32   0.0.0.0          imp-null/exp-null
10.17.17.17/32   10.0.0.1         20/exp-null
10.18.18.18/32   10.0.0.1         24/31
10.18.18.18/32   10.0.0.1         24/33
```

Table 26 describes the significant fields shown in the display.

Table 26 show ip bgp labels Field Descriptions

Field	Description
Network	Displays the network address from the eGBP table.
Next Hop	Specifies the eBGP next hop address.
In Label	Displays the label (if any) assigned by this router.
Out Label	Displays the label assigned by the BGP next hop router.

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.

show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

show ip bgp neighbors [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy** [**detail**]]]

Syntax Description

ip-address	(Optional) IP address of a neighbor. If this argument is omitted, all neighbors are displayed.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths *reg-exp*	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
received prefix-filter	(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the **received-routes** keyword.
policy	(Optional) Displays the policies applied to this neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **received-routes** keyword was added.
12.0(18)S	The output was modified to display the no-prepend configuration option and this command was integrated into Cisco IOS Release 12.0(18)S.
12.2(4)T	The **received** and **prefix-filter** keywords were added, and this command was integrated into Cisco IOS Release 12.2(4)T.

Release	Modification
12.0(21)ST	The output was modified to display Multiprotocol Label Switching (MPLS) label information.
12.0(22)S	Support for the BGP graceful restart capability was integrated into the output. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	Support for the BGP graceful restart capability was integrated into the output.
12.0(25)S	The **policy** and **detail** keywords were added.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.0(27)S	The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.3(7)T	The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.0(31)S	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.2(18)SXE	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(4)T	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the output was modified to support BGP TCP path MTU discovery.
12.4(11)T	Support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	Support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	The output was modified to support BGP dynamic neighbors.

Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, and Later Releases

When BGP neighbors use multiple levels of peer templates, it can be difficult to determine which policies are applied to the neighbor.

In Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer-group or a peer-policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. Examples using the various keywords appear in the following sections:

show ip bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Router# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability:advertised and received
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0
  Number of NLRIs in the update sent: max 0, min 0
```

```
  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

Table 27 describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

Table 27 show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when migrating autonomous systems.
internal link	“internal link” is displayed for iBGP neighbors. “external link” is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hhmmss, that the underlying TCP connection has been in existence.

Table 27 show ip bgp neighbors Field Descriptions (continued)

Field	Description
Last read	Time, in hhmmss, since BGP last received a message from this neighbor.
last write	Time, in hhmmss, since BGP last sent a message to this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. "advertised and received" is displayed when a capability is successfully exchanged between two routers.
Route Refresh	Status of the route refresh capability.
MPLS Label Capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Received	Total number of received messages.
Opens	Number of open messages sent and received.
notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
For address family:	Address family to which the following fields refer.
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
...update-group	Number of update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes current	Number of prefixes accepted for this address family.
Prefixes total	Total number of received prefixes.

Table 27 show ip bgp neighbors Field Descriptions (continued)

Field	Description
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as bestpaths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS-path length policy denials.
* AS_PATH loop	Displays outbound AS-path loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of AS 0.
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound non-local next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress-map.
* advertise-map	Displays inbound denials due to an advertise-map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the bestpath came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.

Table 27 show ip bgp neighbors Field Descriptions (continued)

Field	Description
* Bestpath from iBGP peer	Deploys inbound denials because the bestpath came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a CE router.
* BGP distribute-list	Displays inbound denials due to a distribute list.
Number of NLRIs...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be... (not shown in the display)	Indicates that the BGP TTL security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.

Table 27 show ip bgp neighbors Field Descriptions (continued)

Field	Description
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
out of order:	Number of packets received out of sequence.
with data	Number of update packets received with data.
Last reset	Elapsed time since this peering session was last reset.
unread input bytes	Number of bytes of packets still to be processed.
retransmit	Number of packets retransmitted.
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgements (transmissions before or without subsequent acknowledgements).
Second Congestion	Number of second retransmissions sent due to congestion.

show ip bgp neighbors advertised-routes: Example

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Router# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

Table 28 describes the significant fields shown in the display.

Table 28 show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.

Table 28 show ip bgp neighbors advertised-routes Field Descriptions (continued)

Field	Description
Metric	If shown, this is the value of the inter-autonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp neighbors paths: Example

The following is example output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Router# show ip bgp neighbors 172.29.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

Table 29 describes the significant fields shown in the display.

Table 29 show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

show ip bgp neighbors received prefix-filter: Example

The following example shows that a prefix-list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Router# show ip bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

Table 30 describes the significant fields shown in the display.

Table 30 show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

show ip bgp neighbors policy: Example

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited polices are policies that the neighbor inherits from a peer-group or a peer-policy template.

```
Router# show ip bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

Cisco IOS Release 12.0(31)S and 12.4(4)T: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that Bidirectional Forwarding Detection (BFD) is being used to detect fast fallover for the BGP neighbor that is a BFD peer.

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
.
.
.
 Using BFD to detect fast fallover
```

Cisco IOS Release 12.2(33)SRA: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2.

```
Router# show ip bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

Cisco IOS Release 12.2(33)SXH: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that the neighbor 192.168.3.2 is a member of the peer group, group192, and belongs to the subnet range group 192.168.0.0/16, which shows that this BGP neighbor was dynamically created.

```
Router# show ip bgp neighbors 192.168.3.2

BGP neighbor is *192.168.3.2,  remote AS 50000, external link
 Member of peer-group group192 for session parameters
 Belongs to the subnet range group: 192.168.0.0/16
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:06:35
  Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             7          7
    Route Refresh:          0          0
    Total:                  8          8
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  group192 peer-group member
.
.
.
```

Related Commands

Command	Description
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.

show ip bgp vpnv4

To display Virtual Private Network Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**rib-failure**] [*ip-prefix*/*length* [**longer-prefixes**]] [*network-address* [*mask*] [**longer-prefixes**]] [**cidr-only**] [**community**] [**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**labels**]

Syntax Description

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays Network Layer Reachability Information (NLRI) prefixes that match the named route distinguisher.
vrf *vrf-name*	Displays NLRI prefixes associated with the named VPN routing and forwarding (VRF) instance.
rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
ip-prefix/length	(Optional) IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
network-address	(Optional) IP address of a network in the BGP routing table.
mask	(Optional) Mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonclassful net masks.
community	(Optional) Displays routes that match this community.
community-list	(Optional) Displays routes that match this community list.
dampened-paths	(Optional) Displays paths suppressed because of dampening (BGP route from peer is up and down).
filter-list	(Optional) Displays routes that conform to the filter list.
flap-statistics	(Optional) Displays flap statistics of routes.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
quote-regexp	(Optional) Displays routes that match the autonomous system path regular expression.
regexp	(Optional) Displays routes that match the autonomous system path regular expression.

summary	(Optional) Displays BGP neighbor status.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The output of the **show ip bgp vpnv4 all** *ip-prefix* command was enhanced to display attributes including multipaths and a best path to the specified network.
12.0(21)ST	The **tags** keyword was replaced by the **labels** keyword to conform to the MPLS guidelines. This command was integrated into Cisco IOS Release 12.0(21)ST.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(27)S	The output of the **show ip bgp vpnv4 all labels** command was enhanced to display explicit-null label information.
12.3	The **rib-failure** keyword was added for VRFs.
12.2(22)S	The output of the **show ip bgp vpnv4 vrf** *vrf-name* **labels** command was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(25)S	This command was updated to display MPLS VPN nonstop forwarding information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. The display output was modified to indicate whether BGP Nonstop Routing (NSR) with stateful switchover (SSO) is enabled and the reason the last BGP lost SSO capability.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the output was modified to support per-VRF assignment of the BGP router ID.
12.2(31)SB2	The output was modified to support per-VRF assignment of the BGP router ID.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH, and the output was modified to support per-VRF assignment of the BGP router ID. **Note** In Cisco IOS Release 12.2(33)SXH, the command output does not display on the standby route processor in NSF/SSO mode.
12.4(20)T	The output was modified to support per-VRF assignment of the BGP router ID.
15.0(1)M	This command was modified. The output was modified to support BGP Event-Based VPN Import.
12.2(33)SRE	This command was modified. The command output was modified to support the BGP Event-Based VPN Import, BGP best external and BGP additional path features.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays explicit-null label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32       10.0.0.21               11    100      0 ?
*> 10.7.7.7/32       10.150.0.2              11         32768 ?
*>i10.69.0.0/30      10.0.0.21                0    100      0 ?
*> 10.150.0.0/24     0.0.0.0                  0         32768 ?
```

Table 31 describes the significant fields shown in the display.

Table 31 show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 labels

Network            Next Hop       In label/Out label
Route Distinguisher: 100:1 (vrf1)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

Table 32 describes the significant fields shown in the display.

Table 32 show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.

Table 32 show ip bgp vpnv4 rd labels Field Descriptions (continued)

In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 10.2.2.2/32      192.168.1.1                           0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                 0    100      0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                 0    100      0 100 i
*> 192.168.3.0      192.168.1.1                           0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
```

Table 33 describes the significant fields shown in the display.

Table 33 show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Router# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out nolabel/17
  100, imported path from 300:1:192.168.9.0/24
```

```
10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
  Origin IGP, metric 0, localpref 100, valid, internal, best
  Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
  Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
  mpls labels in/out nolabel/17
```

Table 34 describes the significant fields shown in the display.

Table 34 show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is *internal* if the path is learned via iBGP. The field is *external* if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf xyz rib-failure

Network          Next Hop                    RIB-failure   RIB-NH Matches
```

```
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

Table 35 describes the significant fields shown in the display.

Table 35 show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Note In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature incurred various infrastructure changes. The result of those changes affects the output of this command on the standby Route Processor (RP). In Cisco IOS Release 12.2(33)SXH, the standby RP does not display any output from the **show ip bgp vpnv4** command.

Active Route Processor

```
Router# show ip bgp vpnv4 all labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32   0.0.0.0    18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
```

```
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
```

Standby Route Processor

```
Router# show ip bgp vpnv4 all labels

Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels

Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

Table 36 describes the significant fields shown in the display.

Table 36 show ip bgp vpn4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Router# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24       10.0.0.0        19/aggregate(v1)
   10.0.0.1/32       10.0.0.0        20/nolabel
   10.1.1.1/32       10.0.0.0        21/aggregate(v1)
   10.10.10.10/32    10.0.0.1        25/exp-null
   10.168.100.100/32
                     10.0.0.1        23/exp-null
   10.168.101.101/32
                     10.0.0.1        22/exp-null
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.

Table 37 show ip bgp vpnv4 all labels Field Descriptions (continued)

Field	Description
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output from an image in Cisco IOS Release 12.2(31)SB2, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, Cisco IOS XE Release 2.1, and later releases with the Per-VRF Assignment of BGP Router ID feature configured. The router ID is shown next to the VRF name.

```
Router# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

Table 38 describes the significant fields shown in the display.

Table 38 show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

In this example, the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the bestpath or multipaths are not eligible for import), the imported path includes the wording “imported safety path,” as shown in the output.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

In this example the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does

not match the RTs imported by the specified VRF. In this situation, the imported path is marked as "not-in-vrf" as shown in the output. Note that on the net for vrf-A, this path is not the bestpath as any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
       mpls labels in/out nolabel/16
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip explicit-paths

To display the configured IP explicit paths, use the **show ip explicit-paths** command in user EXEC or privileged EXEC mode.

show ip explicit-paths [**name** *pathname* | **identifier** *number*] [**detail**]

Syntax Description

name *pathname*	(Optional) Displays the pathname of the explicit path.
identifier *number*	(Optional) Displays the number of the explicit path. Valid values are from 1 to 65535.
detail	(Optional) Displays, in the long form, information about the configured IP explicit paths.

Command Default

If you enter the command without entering an optional keyword, all configured IP explicit paths are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	The command output was enhanced to display SLRG-releated information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

Examples

The following is sample output from the **show ip explicit-paths** command:

```
Router# show ip explicit-paths

PATH 200 (strict source route, path complete, generation 6)
    1: next-address 10.3.28.3
    2: next-address 10.3.27.3
```

Table 39 describes the significant fields shown in the display.

Table 39 show ip explicit-paths Field Descriptions

Field	Description
PATH	Pathname or number, followed by the path status.
1: next-address	First IP address in the path.
2: next-address	Second IP address in the path.

Related Commands

Command	Description
append-after	Inserts a path entry after a specific index number.
index	Inserts or modifies a path entry at a specific index.
ip explicit-path	Enters the subcommand mode for IP explicit paths so that you can create or modify the named path.
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.

show ip multicast mpls vif

To display the virtual interfaces (VIFs) that are created on the Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) tailend router, use the **show ip multicast mpls vif** command in privileged EXEC mode.

show ip multicast mpls vif

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example shows information about the virtual interfaces:

```
Router# show ip multicast mpls vif

Interface   Next-hop            Application     Ref-Count   Table / VRF name
 Lspvif0     10.1.0.1            Traffic-eng      1           default
 Lspvif4     10.2.0.1            Traffic-eng      1           default
```

Table 40 describes the significant fields shown in the display.

Table 40 show ip multicast mpls vif Field Descriptions

Field	Description
Interface	The name of the virtual interface
Next-hop	For P2MP TE, the source address of the TE P2MP tunnel. Only one label switched path (LSP) VIF is created for all TE P2MP tunnels that have the same source address.
Application	The name of the multicast application that creates the VIF.
Table/VRF name	The multicast virtual routing and forwarding (VRF) table used.

Related Commands

Command	Description
show ip mroute	Displays IP multicast traffic.

show ip ospf database opaque-area

To display lists of information related to traffic engineering opaque link-state advertisements (LSAs), also known as Type-10 opaque link area link states, use the **show ip ospf database opaque-area** command in user EXEC or privileged EXEC mode.

show ip ospf database opaque-area

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(8)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip ospf database opaque-area** command:

```
Router# show ip ospf database opaque-area

OSPF Router with ID (10.3.3.3) (Process ID 1)

                Type-10 Opaque Link Area Link States (Area 0)

  LS age: 12
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 10.0.0.0
  Opaque Type: 1
  Opaque ID: 0
  Advertising Router: 172.16.8.8
  LS Seq Number: 80000004
  Checksum: 0xD423
  Length: 132
  Fragment number : 0

    MPLS TE router ID: 172.16.8.8

    Link connected to Point-to-Point network
      Link ID : 10.2.2.2

      Interface Address : 192.168.1.1
```

Table 41 describes the significant fields shown in the display.

Table 41 show ip ospf database opaque-area Field Descriptions

Field	Description
LS age	Link-state age.
Options	Type of service options.
LS Type	Type of the link state.
Link State ID	Router ID number.
Opaque Type	Opaque link-state type.
Opaque ID	Opaque LSA ID number.
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence number that detects old or duplicate link state advertisements (LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.
Length	Length (in bytes) of the LSA.
Fragment number	Arbitrary value used to maintain multiple traffic engineering LSAs.
MPLS TE router ID	Unique MPLS traffic engineering ID.
Link ID	Index of the link being described.
Interface Address	Address of the interface.

Related Commands

Command	Description
mpls traffic-eng area	Configures a router running OSPF MPLS to flood traffic engineering for an indicated OSPF area.
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
show ip ospf mpls traffic-eng	Provides information about the links available on the local router for traffic engineering.

show ip ospf mpls ldp interface

To display information about interfaces belonging to an Open Shortest Path First (OSPF) process that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP), use the **show ip ospf mpls ldp interface** command in privileged EXEC mode.

show ip ospf [*process-id*] **mpls ldp interface** [*interface*]

Syntax Description

process-id	(Optional) Process ID. Includes information only for the specified routing process.
interface	(Optional) Defines the interface for which MPLS LDP-IGP synchronization information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command shows MPLS LDP-IGP synchronization information for specified interfaces or OSPF processes. If you do not specify an argument, information is displayed for each interface that was configured for MPLS LDP-IGP synchronization.

Examples

The following is sample output from the **show ip ospf mpls ldp interface** command:

```
Router# show ip ospf mpls ldp interface

Serial1/2.4
  Process ID 2, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holddown timer is disabled
  Interface is up
Serial1/2.11
  Process ID 6, VRF VFR1, Area 2
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holddown timer is disabled
  Interface is up
Ethernet2/0
  Process ID 1, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Required
  Holddown timer is configured : 1 msecs
  Holddown timer is not running
```

```
  Interface is up
Loopback1
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holddown timer is disabled
  Interface is up
Serial1/2.1
  Process ID 1, Area 10.0.1.44
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Required
  Holddown timer is configured : 1 msecs
  Holddown timer is not running
  Interface is up
```

Table 42 describes the significant fields shown in the display.

Table 42 show ip ospf mpls ldp interface Field Descriptions

Field	Description
Process ID	The number of the OSPF process to which the interface belongs.
Area	The OSPF area to which the interface belongs.
LDP is configured through	The means by which LDP was configured on the interface. LDP can be configured on the interface by the **mpls ip** or **mpls ldp** command.
LDP-IGP Synchronization	Indicates whether MPLS LDP-IGP synchronization was enabled on this interface.
Holddown timer	Indicates whether the hold-down timer was specified for this interface.

Related Commands

Command	Description
debug mpls ldp igp sync	Displays events related to MPLS LDP-IGP synchronization.
show mpls ldp igp sync	Displays the status of the MPLS LDP-IGP synchronization process.

show ip ospf mpls traffic-eng

To display information about the links available on the local router for traffic engineering, use the **show ip ospf mpls traffic-eng** command in user EXEC or privileged EXEC mode.

show ip ospf [**process-id** [**area-id**] **mpls traffic-eng** [**link**] | **fragment**]

Syntax Description

process-id	(Optional) Internal identification number that is assigned locally when the OSPF routing process is enabled. The value can be any positive integer.
area-id	(Optional) Area number associated with OSPF.
link	(Optional) Provides detailed information about the links over which traffic engineering is supported on the local router.
fragment	(Optional) Provides detailed information about the traffic engineering fragments on the local router.

Defaults

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip ospf mpls traffic-eng** command:

```
Router# show ip ospf mpls traffic-eng link

OSPF Router with ID (10.0.0.1) (Process ID 1)

  Area 0 has 2 MPLS TE links. Area instance is 14.

  Links in hash bucket 8.
    Link is associated with fragment 1. Link instance is 14
      Link connected to Point-to-Point network
      Link ID :197.0.0.1
      Interface Address :172.16.0.1
      Neighbor Address :172.16.0.2
      Admin Metric :97
```

```
  Maximum bandwidth :128000
  Maximum reservable bandwidth :250000
  Number of Priority :8
  Priority 0 :250000      Priority 1 :250000
  Priority 2 :250000      Priority 3 :250000
  Priority 4 :250000      Priority 5 :250000
  Priority 6 :250000      Priority 7 :212500
  Affinity Bit :0x0
Link is associated with fragment 0. Link instance is 14
  Link connected to Broadcast network
  Link ID :192.168.1.2
  Interface Address :192.168.1.1
  Neighbor Address :192.168.1.2
  Admin Metric :10
  Maximum bandwidth :1250000
  Maximum reservable bandwidth :2500000
  Number of Priority :8
  Priority 0 :2500000     Priority 1 :2500000
  Priority 2 :2500000     Priority 3 :2500000
  Priority 4 :2500000     Priority 5 :2500000
  Priority 6 :2500000     Priority 7 :2500000
  Affinity Bit :0x0
```

Table 43 describes the significant fields shown in the display.

Table 43 show ip ospf mpls traffic-eng Field Descriptions

Field	Description
OSPF Router with ID	Router identification number.
Process ID	OSPF process identification.
Area instance	Number of times traffic engineering information or any link changed.
Link instance	Number of times any link changed.
Link ID	Link-state ID.
Interface Address	Local IP address on the link.
Neighbor Address	IP address that is on the remote end of the link.
Admin Metric	Traffic engineering link metric.
Maximum bandwidth	Bandwidth set by the **bandwidth interface** command in the interface configuration mode.
Maximum reservable bandwidth	Bandwidth available for traffic engineering on this link. This value is set in the **ip rsvp** command in the interface configuration mode.
Number of priority	Number of priorities that are supported.
Priority	Bandwidth (in bytes per second) that is available for traffic engineering at certain priorities.
Affinity Bit	Affinity bits (color) assigned to the link.

show ip protocols vrf

To display the routing protocol information associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ip protocols vrf** command in user EXEC or privileged EXEC mode.

show ip protocols vrf *vrf-name* **summary**

Syntax Description

vrf-name	Name assigned to a VRF.
summary	Displays the routing protocol information in summary format.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	The **summary** keyword was added. EIGRP VRF support was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display routing information associated with a VRF.

Examples

The following example shows information about a VRF named vpn1:

```
Router# show ip protocols vrf vpn1

Routing Protocol is "bgp 100"
  Sending updates every 60 seconds, next due in 0 sec
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Redistributing:connected, static
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.13.13.13          200      02:20:54
    10.18.18.18          200      03:26:15
  Distance:external 20 internal 200 local 200
```

Table 44 describes the significant fields shown in the display.

Table 44 show ip protocols vrf Field Descriptions

Field	Description
Gateway	Displays the IP address of the router identifier for all routers in the network.
Distance	Displays the metric used to access the destination route.
Last Update	Displays the last time the routing table was updated from the source.

Related Commands

Command	Description
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip route

To display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]

Syntax Description

ip-address	(Optional) Address about which routing information should be displayed.
mask	(Optional) Argument for a subnet mask.
longer-prefixes	(Optional) Specifies that only routes matching the *ip-address* and *mask* pair should be displayed.
protocol	(Optional) The name of a routing protocol, or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **hello**, **eigrp**, **isis**, **odr**, **ospf**, and **rip**.
process-id	(Optional) The number used to identify a process of the specified protocol.
list	(Optional) The list keyword is required to filter output by an access list name or number.
access-list-number	(Optional) Filters the displayed output from the routing table based on the specified access list name.
access-list-name	(Optional) Filters the displayed output from the routing table based on the specified access list number.
static	(Optional) All static routes.
download	(Optional) The route installed using the AAA route download function. This keyword is used only when AAA is configured.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
9.2	This command was introduced.
10.0	The “D—EIGRP, EX—EIGRP, N1—OSPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were added to the command output.
10.3	The *process-id* argument was added.
11.0	The **longer-prefixes** keyword was added.
11.1	The “U—per-user static route” code was added to the command output.
11.2	The “o—on-demand routing” code was added to the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
11.3	The output from the **show ip route** *ip-address* command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	The "M—mobile" code was added to the command output.
12.0(3)T	The "P—periodic downloaded static route" code was added to the command output.
12.0(4)T	The "ia—IS-IS" code was added to the command output.
12.2(2)T	The output from the **show ip route** *ip-address* command was enhanced to display information on the multipaths to the specified network.
12.2(13)T	The *egp* and *igrp* arguments were removed because the exterior gateway protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) are no longer available in Cisco IOS software.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	The output was enhanced to display route tag information.
12.3(8)T	The output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **show ip route static download** command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **show ip route** and **show ip route static** commands after these active routes are added in the main routing table.

Examples

Routing Table Examples

The following examples show the standard routing tables displayed by the **show ip route** command. Use the codes displayed at the beginning of each report and the information in Table 45 to understand the type of route.

The following is sample output from the **show ip route** command when entered without an address:

```
Router# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
```

```
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following is sample output that includes IS-IS Level 2 routes learned:

```
Router# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

     10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       10.89.64.0 255.255.255.0 is possibly down,
          routing via 0.0.0.0, Ethernet0
i L2    10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2    10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
```

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
```

```
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
Router# show ip route

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, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 172.21.17.1 to network 0.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Router# show ip route static

     172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.27.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.21.114.201/32 is directly connected, BRI0
S       172.21.114.205/32 is directly connected, BRI0
S       172.21.114.174/32 is directly connected, BRI0
S       172.21.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/8 is directly connected, BRI0
P    10.2.2.0/8 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
S    172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

The following example shows how to use the **show ip route static download** command to display all active and inactive routes installed using AAA route download:

```
Router# show ip route static download

Connectivity: A - Active, I - Inactive

A     10.10.0.0 255.0.0.0 BRI0
A     10.11.0.0 255.0.0.0 BRI0
A     10.12.0.0 255.0.0.0 BRI0
A     10.13.0.0 255.0.0.0 BRI0
I     10.20.0.0 255.0.0.0 172.21.1.1
```

```
I     10.22.0.0 255.0.0.0 Serial0
I     10.30.0.0 255.0.0.0 Serial0
I     10.31.0.0 255.0.0.0 Serial1
I     10.32.0.0 255.0.0.0 Serial1
A     10.34.0.0 255.0.0.0 192.168.1.1
A     10.36.1.1 255.255.255.255 BRI0 200 name remote1
I     10.38.1.9 255.255.255.0 192.168.69.1
```

Table 45 show ip route Field Descriptions

Field	Description
O	Indicates the protocol that derived the route. It can be one of the following values: R—Routing Information Protocol (RIP) derived O—Open Shortest Path First (OSPF) derived C—connected S—static B—Border Gateway Protocol (BGP) derived D—Enhanced Interior Gateway Routing Protocol (EIGRP) EX—EIGRP external i—IS-IS derived ia—IS-IS M—mobile P—periodic downloaded static route U—per-user static route o—on-demand routing
E2	Type of route. It can be one of the following values: *—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. IA—OSPF interarea route E1—OSPF external type 1 route E2—OSPF external type 2 route L1—IS-IS Level 1 route L2—IS-IS Level 2 route N1—OSPF not-so-stubby area (NSSA) external type 1 route N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.

Table 45 show ip route Field Descriptions (continued)

Field	Description
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Specific Route Information

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the IP address 10.0.0.1:

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
    Known via “isis”, distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The example above shows the output from the **show ip route** command when looking at an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

Table 46 describes the significant fields shown when using the **show ip route** command with an IP address.

Table 46 show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0

Routing entry for 10.22.0.0/16
  Known via “isis”, distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
        Route metric is 12, traffic share count is 1
        Route tag 120
```

Static Routes Using a DHCP Gateway Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

```
Router# show ip route

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, su - IS-IS summary, 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 10.0.19.14 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.
show interfaces tunnel	Displays a list of tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip route vrf

To display the IP routing table associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [*ip-prefix*] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]]

Syntax Description

vrf-name	Name assigned to the VRF.
connected	(Optional) Displays all connected routes in a VRF.
protocol	(Optional) To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
tag	(Optional) Cisco IOS routing area label.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
ip-prefix	(Optional) Specifies a network to display.
list *number*	(Optional) Specifies the IP access list to display.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
supernets-only	(Optional) Displays supernet entries only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The *ip-prefix* argument was added. The output from the **show ip route vrf** *vrf-name ip-prefix* command was enhanced to display information on the multipaths to the specified network.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) VRF support was added.
12.2(15)T	EIGRP VRF support was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP VRF support was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The output was enhanced to display remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the Routing Information Base (RIB).

Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

Examples

This example shows the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1

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, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This example shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1 bgp

B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

This example shows the IP routing table associated with a VRF named PATH and network 10.22.22.0:

```
Router# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

Table 47 describes the significant fields shown when the **show ip route vrf** *vrf-name ip-prefix* command is used.

Table 47 show ip route vrf Field Descriptions

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	The metric to reach the destination network.
Tag	Integer that is used to implement the route.
type	Indicates that the route is an L1 type or L2 type route.
Last update from 10.22.5.10	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
00:01:07 ago	Specifies the last time the route was updated (in hours:minutes:seconds).
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
10.22.6.10, from 10.11.6.7, 00:01:07 ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.
AS Hops	Number of hops to the destination or to the router where the route first enters internal BGP (iBGP).

Example of Output Using the Cisco IOS Software Modularity for Layer 3 VPNs Feature

The following is sample output from the **show ip route vrf** command on routers using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB, if BGP is the label distribution protocol:

```
Router# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

Table 48 describes the significant fields shown in the display.

Table 48 show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16 - 1048575) • A reserved label value, such as explicit-null or implicit-null • The word “none” if no label is received from the peer The MPLS label field does not display if any of the following conditions is true: • BGP is not the LDP. However, OSPF prefixes learned via sham link display an MPLS label. • MPLS is not supported. • The prefix was imported from another VRF, where the prefix was an IGP prefix and LDP provided the remote label for it.
MPLS Flags	The name of one of the following MPLS flags is displayed if any is set: • MPLS Required—Packets are forwarded to this prefix because the MPLS label stack is present. If MPLS is disabled in the outgoing interface, the packets are dropped. • No Global—MPLS packets for this prefix are forwarded from the VRF interface, not from the interface in global table. Using the VRF interface prevents loops in scenarios that use ieBGP multipath. • NSF—The prefix is from an NSF-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.

Related Commands

Command	Description
show ip cache	Displays the Cisco Express Forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip rsvp fast bw-protect

To display information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection, use the **show ip rsvp fast bw-protect** command in user EXEC or privileged EXEC mode.

show ip rsvp fast bw-protect

Syntax Description

This command has no arguments or keywords.

Command Default

The backup bandwidth protection and backup tunnel status information is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip rsvp fast bw-protect** command:

```
Router# show ip rsvp fast bw-protect

Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
--------------   -------  --------   ----------    -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

Table 49 describes the significant fields shown in the display.

Table 49 show ip rsvp fast bw-protect Field Descriptions

Field	Description
Primary Tunnel	Identification of the tunnel being protected.
Protect I/F	Interface name.

Table 49 show ip rsvp fast bw-protect Field Descriptions (continued)

Field	Description
BW BPS:Type	Bandwidth, in bits per second, and type of bandwidth. Possible values are: • S—Subpool • G—Global pool
Backup Tunnel:Label	Identification of the backup tunnel.
State	Status of backup tunnel. Valid values are: • Ready—Data is passing through the primary tunnel, but the backup tunnel is ready to take over if the primary tunnel goes down. • Active—The primary tunnel is down, so the backup tunnel is used for traffic. • None—There is no backup tunnel.
BW-P	Status of backup bandwidth protection. Possible values are ON and OFF.
Type	Type of backup tunnel. Possible values are: • Nhop—Next hop • NNHOP—Next-next hop

Related Commands

Command	Description
tunnel mpls traffic-eng fast-reroute bw-protect	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

show ip rsvp fast detail

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **show ip rsvp fast detail** command in user EXEC or privileged EXEC mode.

show ip rsvp fast detail

Syntax Description

This command has no arguments or keywords.

Command Default

Specific information for RSVP categories is not displayed.

Command Modes

User EXEC
Privileged EXEC'

Command History

Release	Modification
12.0(24)S	This command was introduced
12.0(29)S	Bandwidth Prot desired was added in the Flag field of the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip rsvp fast detail** command:

```
Router# show ip rsvp fast detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: PRAB-72-5_t500
  ERO: (incoming)
    10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
    555.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    555.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    555.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    555.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: Ready -- backup tunnel selected
      Backup Tunnel: Tu501      (label 19)
      Bkup Sender Template:
        Tun Sender: 555.5.6.5  LSP ID: 8
```

```
    Bkup FilerSpec:
      Tun Sender: 555.5.6.5, LSP ID: 8
Path ID handle: 04000405.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

Table 50 describes the significant fields shown in the display.

Table 50 show ip rsvp fast detail Field Descriptions

Field	Description
Tun Dest	IP address of the receiver.
Tun ID	Tunnel identification number.
Ext Tun ID	Extended tunnel identification number.
Tun Sender	IP address of the sender.
LSP ID	Label-switched path identification number.
Setup Prio	Setup priority.
Holding Prio	Holding priority.
Flags	Backup bandwidth protection has been configured for the label-switched path (LSP).
Session Name	Name of the session.
ERO (incoming)	EXPLICIT_ROUTE object of incoming path messages.
ERO (outgoing)	EXPLICIT_ROUTE object of outgoing path messages.
Traffic params Rate	Average rate, in bits per second.
Max. burst	Maximum burst size, in bytes.
Min Policed Unit	Minimum policed units, in bytes.
Max Pkt Size	Maximum packet size, in bytes.
Inbound FRR	Status of inbound Fast Reroute (FRR) backup tunnel. If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active.
Outbound FRR	Status of outbound FRR backup tunnel. If this node is a point of local repair (PLR) for an LSP, there are three possible states: • Active—This LSP is actively using its backup tunnel, presumably because there has been a downstream failure. • No Backup—This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure. • Ready—This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use.

Table 50 show ip rsvp fast detail Field Descriptions (continued)

Field	Description
Backup Tunnel	If the Outbound FRR state is Ready or Active, this field indicates the following: • Which backup tunnel has been selected for this LSP to use in case of a failure. • The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point).
Bkup Sender Template	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Bkup FilerSpec	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Path ID handle	Protection Switch Byte (PSB) identifier.
Incoming policy	Policy decision of the LSP. If RSVP policy was not granted for the incoming path message for the tunnel, the LSP does not come up. Accepted is displayed.
Policy source(s)	For FRR LSPs, this value always is MPLS/TE for the policy source.
Status	For FRR LSPs, valid values are: • Proxied—Headend routers • Proxied Terminated—Tailend routers For midpoint routers, the field always is blank.

Related Commands

Command	Description
mpls traffic-eng fast-reroute backup-prot-preemption	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted.

show ip rsvp hello

To display hello status and statistics for Fast Reroute, reroute (hello state timer), and graceful restart, use the **show ip rsvp hello** command in user EXEC or privileged EXEC mode.

show ip rsvp hello

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The command output was modified to include graceful restart, reroute (hello state timer), and Fast Reroute information.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	The command output was modified to show whether graceful restart is configured and full mode was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	The command output was modified to include Bidirectional Forwarding Detection (BFD) protocol information.

Examples

The following is sample output from the **show ip rsvp hello** command:

```
Router# show ip rsvp hello

Hello:
 RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
 BFD for Fast-Reroute/Reroute: Enabled
 RSVP Hello for Graceful Restart: Disabled
```

Table 51 describes the significant fields shown in the display. The fields describe the processes for which hello is enabled or disabled.

Table 51 show ip rsvp hello Field Descriptions

Field	Description
RSVP Hello for Fast-Reroute/Reroute	Status of Fast-Reroute/Reroute: • Enabled—Fast reroute and reroute (hello for state timer) are activated (enabled). • Disabled—Fast reroute and reroute (hello for state timer) are not activated (disabled).
Statistics	Status of hello statistics: • Enabled—Statistics are configured. Hello packets are time-stamped when they arrive in the hello input queue for the purpose of recording the time required until they are processed. • Disabled—Hello statistics are not configured. • Shutdown—Hello statistics are configured but not operational. The input queue is too long (that is, more than 10,000 packets are queued).
BFD for Fast-Reroute/Reroute	Status of BFD for Fast-Reroute/Reroute: • Enabled—BFD is configured. • Disabled—BFD is not configured.
Graceful Restart	Restart capability: • Enabled—Restart capability is activated for a router (full mode) or its neighbor (help-neighbor). • Disabled—Restart capability is not activated.

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on the router.
ip rsvp signalling hello statistics	Enables hello statistics on the router.
show ip rsvp hello statistics	Displays how long hello packets have been in the hello input queue.

show ip rsvp hello bfd nbr

To display information about all Multiprotocol Label Switching (MPLS) traffic engineering (TE) clients that use the Bidirectional Forwarding Detection (BFD) protocol, use the **show ip rsvp hello bfd nbr** command in user EXEC or privileged EXEC mode.

show ip rsvp hello bfd nbr

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

The command output is the same as the **show ip rsvp hello bfd nbr summary** command output.

Examples

The following is sample output from the **show ip rsvp hello bfd nbr** command.

```
Router# show ip rsvp hello bfd nbr

Client  Neighbor    I/F     State  LostCnt  LSPs
FRR     10.0.0.6    Gi9/47  Up     0        1
```

Table 52 describes the significant fields shown in the display.

Table 52 show ip rsvp hello bfd nbr Field Descriptions

Field	Description
Client	MPLS TE feature that is using the BFD protocol.
Neighbor	IP address of the next-hop (that is, the neighbor).
I/F	Outbound (egress) interface name.
State	Status of the BFD session (Up, Down, or Lost).
LostCnt	Number of times that the BFD session is lost (dropped) on this interface.
LSPs	Number of label-switched paths (LSPs) that BFD is protecting on this interface.

Related Commands

Command	Description
clear ip rsvp hello bfd	Globally resets to zero the number of times that the BFD protocol was dropped on an interface or the number of times that a link was down.
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol globally on the router for MPLS TE link and node protection.
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol on an interface for MPLS TE link and node protection.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

show ip rsvp hello bfd nbr detail

To display detailed information about all Multiprotocol Label Switching (MPLS) traffic engineering (TE) clients that use the Bidirectional Forwarding Detection (BFD) protocol, use the **show ip rsvp hello bfd nbr detail** command in user EXEC or privileged EXEC mode.

show ip rsvp hello bfd nbr detail

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Examples

The following is sample output from the **show ip rsvp hello bfd nbr detail** command:

```
Router# show ip rsvp hello bfd nbr detail

 Hello Client Neighbors

 Remote addr 10.0.0.6, Local addr  10.0.0.7
  Type: Active
  I/F: Gi9/47
  State: Up (for 00:09:41)
  Clients: FRR
  LSPs protecting: 1 (frr: 1, hst upstream: 0 hst downstream: 0)
  Communication with neighbor lost: 0
```

Table 53 describes the significant fields shown in the display.

Table 53 show ip rsvp hello bfd nbr detail Field Descriptions

Field	Description
Remote addr	IP address of the next hop interface.
Local addr	IP address of the outbound interface.
Type	Type of signaling that is in effect (Active or Passive).
I/F	Interface name.
State	Status of the BFD session (Up, Down, or Lost).
Clients	Software that is using the BFD protocol.
LSPs protecting	Number of label-switched paths (LSPs) that the BFD protocol is protecting.
Communication with neighbor lost	Number of times the BFD protocol detected that a link was down.

Related Commands

Command	Description
clear ip rsvp hello bfd	Globally resets to zero the number of times that the BFD protocol was dropped on an interface or the number of times that a link was down.
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol globally on the router for MPLS TE link and node protection.
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol on an interface for MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

show ip rsvp hello bfd nbr summary

To display summarized information about all Multiprotocol Label Switching (MPLS) traffic engineering (TE) clients that use the Bidirectional Forwarding Detection (BFD) protocol, use the **show ip rsvp hello bfd nbr summary** command in user EXEC or privileged EXEC mode.

show ip rsvp hello bfd nbr summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXE C

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

The command output is the same as the **show ip rsvp hello bfd nbr** command output.

Examples

The following is sample output from the **show ip rsvp hello bfd nbr summary** command.

```
Router# show ip rsvp hello bfd nbr summary

Client  Neighbor   I/F     State  LostCnt  LSPs
FRR     10.0.0.6   Gi9/47  Up     0        1
```

Table 54 describes the significant fields shown in the display.

Table 54 show ip rsvp hello bfd nbr summary Field Descriptions

Field	Description
Client	MPLS TE feature that uses the BFD protocol.
Neighbor	IP address of the next hop (that is, the neighbor).
I/F	Interface type and slot or port.
State	Status of the BFD session (Up, Down, or Lost).
LostCnt	Number of times that the BFD session is lost (dropped) on this interface.
LSPs	Number of label-switched paths (LSPs) that BFD is protecting on this interface.

Related Commands

Command	Description
clear ip rsvp hello bfd	Globally resets to zero the number of times that the BFD protocol was dropped on an interface or the number of times that a link was down.
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol globally on the router for MPLS TE link and node protection.
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol globally on an interface for MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.

show ip rsvp hello instance detail

To display detailed information about a hello instance, use the **show ip rsvp hello instance detail** command in user EXEC or privileged EXEC mode.

show ip rsvp hello instance detail [**filter destination** *ip-address*]

Syntax Description

filter destination *ip-address*	(Optional) IP address of the neighbor node.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The command output was modified to include graceful restart, hello state timer (reroute), and fast reroute information.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **show ip rsvp hello instance detail** command to display information about the processes (clients) currently configured.

Examples

The following is sample output from the **show ip rsvp hello instance detail** command:

```
Router# show ip rsvp hello instance detail

Neighbor 10.0.0.3  Source  10.0.0.2
    Type: Active    (sending requests)
    I/F:  Serial2/0
    State:   Up        (for 2d19h2d19h)
    Clients: ReRoute
    LSPs protecting: 1
    Missed acks: 4, IP DSCP: 0x30
    Refresh Interval (msec)
      Configured: 6000
      Statistics: (from 40722 samples)
        Min:      6000
        Max:      6064
        Average:  6000
        Waverage: 6000 (Weight = 0.8)
        Current:  6000
    Last sent Src_instance: 0xE617C847
    Last recv nbr's Src_instance: 0xFEC28E95
    Counters:
      Communication with neighbor lost:
        Num times:                    0
        Reasons:
```

```
        Missed acks:                0
        Bad Src_Inst received:      0
        Bad Dst_Inst received:      0
        I/F went down:              0
        Neighbor disabled Hello:    0
    Msgs Received:   55590
         Sent:       55854
         Suppressed: 521

Neighbor 10.0.0.8 Source  10.0.0.7
  Type: Passive   (responding to requests)
  I/F:  Serial2/1
  Last sent Src_instance: 0xF7A80A52
  Last recv nbr's Src_instance: 0xD2F1B7F7
  Counters:
    Msgs Received:   199442
         Sent:       199442
```

Table 55 describes the significant fields shown in the display.

Table 55 show ip rsvp hello instance detail Field Descriptions

Field	Description
Neighbor	IP address of the adjacent node.
Source	IP address of the node that is sending the hello message.
Type	Values are Active (node is sending a request) and Passive (node is responding to a request).
I/F	Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface.
State	Status of communication. Values are as follows: • Up—Node is communicating with its neighbor. • Lost—Communication has been lost. • Init—Communication is being established.
Clients	Clients that created this hello instance; they include graceful restart, ReRoute (hello state timer), and Fast Reroute.
LSPs protecting	Number of LSPs that are being protected by this hello instance.
Missed acks	Number of times that communication was lost due to missed acknowledgments (ACKs).
IP DSCP	IP differentiated services code point (DSCP) value used in the hello IP header.
Refresh Interval (msec)	The frequency (in milliseconds) with which a node generates a hello message containing a Hello Request object for each neighbor whose status is being tracked.
Configured	Configured refresh interval.
Statistics	Refresh interval statistics from a specified number of samples (packets).
Min	Minimum refresh interval.
Max	Maximum refresh interval.

Table 55 show ip rsvp hello instance detail Field Descriptions (continued)

Field	Description
Average	Average refresh interval.
Waverage	Weighted average refresh interval.
Current	Current refresh interval.
Last sent Src_instance	The last source instance sent to a neighbor.
Last recv nbr's Src_instance	The last source instance field value received from a neighbor. (0 means none received.)
Counters	Incremental information relating to communication with a neighbor.
Num times	Total number of times that communication with a neighbor was lost.
Reasons	Subsequent fields designate why communication with a neighbor was lost.
Missed acks	Number of times that communication was lost due to missed ACKs.
Bad Src_Inst received	Number of times that communication was lost due to bad source instance fields.
Bad Dst_Inst received	Number of times that communication was lost due to bad destination instance fields.
I/F went down	Number of times that the interface became unoperational.
Neighbor disabled Hello	Number of times that a neighbor disabled hello messages.
Msgs Received	Number of messages that were received.
Sent	Number of messages that were sent.
Suppressed	Number of messages that were suppressed due to optimization.

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on the router.
ip rsvp signalling hello statistics	Enables hello statistics on the router.
show ip rsvp hello	Displays hello status and statistics for Fast reroute, reroute (hello state timer), and graceful restart.
show ip rsvp hello instance summary	Displays summary information about a hello instance.

show ip rsvp hello instance summary

To display summary information about a hello instance, use the **show ip rsvp hello instance summary** command in user EXEC or privileged EXEC mode.

show ip rsvp hello instance summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The command output was modified to include graceful restart, reroute (hello state timer), and fast reroute information.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following is sample output from the **show ip rsvp hello instance summary** command:

```
Router# show ip rsvp hello instance summary

Active Instances:
  Client  Neighbor        I/F        State      LostCnt  LSPs Interval
  RR      10.0.0.3        Se2/0      Up               0     1 6000
  GR      10.1.1.1        Any        Up              13     1 10000
  GR      10.1.1.5        Any        Lost             0     1 10000
  GR      10.2.2.1        Any        Init             1     0 5000

Passive Instances:
  Neighbor        I/F
  10.0.0.1        Se2/1

Active = Actively tracking neighbor state on behalf of clients:
         RR = ReRoute, FRR = Fast ReRoute, or GR = Graceful Restart
Passive = Responding to hello requests from neighbor
```

Table 56 describes the significant fields shown in the display.

Table 56 show ip rsvp hello instance summary Field Descriptions

Field	Description
Active Instances	Active nodes that are sending hello requests.
Client	Clients on behalf of which hellos are sent; they include GR (graceful restart), RR (reroute = hello state timer), and FRR (Fast Reroute).

Table 56 show ip rsvp hello instance summary Field Descriptions (continued)

Field	Description
Neighbor	IP address of the adjacent node. For graceful restart, this is the neighbor router's ID; for Fast Reroute and hello state timer (reroute), this is one of the neighbor's interface addresses.
I/F	Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface.
State	Status of communication. Values are as follows: • Up—Node is communicating with its neighbor. • Lost—Communication has been lost. • Init—Communication is being established.
LostCnt	Number of times that communication was lost with the neighbor.
LSPs	Number of label-switched paths (LSPs) protected by this hello instance.
Interval	Hello refresh interval in milliseconds.
Passive Instances	Passive nodes that are responding to hello requests.
Neighbor	IP address of adjacent node. For graceful restart, this is the neighbor router's ID; for Fast Reroute and hello state timer (reroute), this is one of the neighbor's interface addresses.
I/F	Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface.

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables hello globally on the router.
ip rsvp signalling hello statistics	Enables hello statistics on the router.
show ip rsvp hello	Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart.
show ip rsvp hello instance detail	Displays detailed information about a hello instance.

show ip rsvp hello statistics

To display how long hello packets have been in the Hello input queue, use the **show ip rsvp hello statistics** command in privileged EXEC mode.

show ip rsvp hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Information about how long hello packets have been in the Hello input queue is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

You can use this command to determine if the Hello refresh interval is too small. If the interval is too small, communication may falsely be declared as lost.

Examples

The following is sample output from the **show ip rsvp hello statistics** command:

```
Router# show ip rsvp hello statistics

Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525
```

Table 57 describes the significant fields shown in the display.

Table 57 show ip rsvp hello statistics Field Descriptions

Field	Description
Status	Indicator of whether Hello has been enabled globally on the router.
Current	Amount of time, in milliseconds, that the current hello packet has been in the Hello input queue.

Table 57 show ip rsvp hello statistics Field Descriptions (continued)

Field	Description
Average	Average amount of time, in milliseconds, that hello packets are in the Hello input queue.
Max	Maximum amount of time, in milliseconds, that hello packets have been in the Hello input queue.
Current length	Current amount of time, in milliseconds, that hello packets have been in the Hello input queue.
Number of samples taken	Number of packets for which these statistics were compiled.

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.
clear ip rsvp hello statistics	Globally clears Hello statistics.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

show ip rsvp high-availability database

To display the contents of the Resource Reservation Protocol (RSVP) high availability (HA) read and write databases used in traffic engineering (TE), use the **show ip rsvp high-availability database** command in user EXEC or privileged EXEC mode.

show ip rsvp high-availability database {**hello** | **link-management** {**interfaces** | **system**} | **lsp** [**filter destination** *ip-address* | **filter lsp-id** *lsp-id* | **filter source** *ip-address* | **filter tunnel-id** *tunnel-id*] | **lsp-head** [**filter** *number*] | **summary**}

Syntax Description

hello	Displays information about the hello entries in the read and write databases.
link-management	Displays information about the link-management entries in the read and write databases.
interfaces	Displays information about the link-management interfaces in the read and write databases.
system	Displays information about the link-management system in the read and write databases.
lsp	Displays information about the label-switched path (LSP) entries in the read and write databases.
filter destination *ip-address*	(Optional) Displays filtered information on the IP address of the destination (tunnel tail).
filter lsp-id *lsp-id*	(Optional) Displays filtered information on a specific LSP ID designated by a number from 0 to 65535.
filter source *ip-address*	(Optional) Displays filtered information on the IP address of the source (tunnel head).
filter tunnel-id *tunnel-id*	(Optional) Displays filtered information on a specific tunnel ID designated by a number from 0 to 65535.
lsp-head	Displays information about the LSP-headend entries in the read and write databases.
filter *number*	(Optional) Displays filtered information on a specific LSP-head router designated by a number from 0 to 65535.
summary	Displays cumulative information about the entries in the read and write databases.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SRB	The command output was modified to display the result of a loose hop expansion performed on the router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC. The command output was modified to include path protection information if you specify the **lsp-head** keyword.

Usage Guidelines

Use the **show ip rsvp high-availability database** command to display information about the entries in the read and write databases.

Use the **show ip rsvp high-availability database lsp** command to display loose hop information. A loose hop expansion can be performed on a router when the router processes the explicit router object (ERO) for an incoming path message. After the router removes all local IP addresses from the incoming ERO, it finds the next hop. If the ERO specifies that the next hop is loose instead of strict, the router consults the TE topology database and routing to determine the next hop and output interface to forward the path message. The result of the calculation is a list of hops; that list is placed in the outgoing ERO and checkpointed with the LSP data as the loose hop information.

Use the **show ip rsvp high-availability database lsp-head** command on a headend router only. On other routers, this command gives no information.

Examples

Hello Example on Active RP

The following is sample output from the **show ip rsvp high-availability database hello** command on an active Route Processor (RP):

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865

HELLO READ DB
```

Table 58 describes the significant fields shown in the displays.

Table 58 show ip rsvp high-availability database hello—Active RP Field Descriptions

Field	Description
HELLO WRITE DB	Storage area for active RP hello data consisting of checkpointed RSVP-TE information that is sent to the standby RP when it becomes the active RP and needs to recover LSPs. This field is blank on a standby RP.
Header	Header information.

Table 58 show ip rsvp high-availability database hello—Active RP Field Descriptions (continued)

Field	Description
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent, but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an acknowledgment (ack) of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Numbers used by the active and standby RPs to synchronize message acks and negative acknowledgments (nacks) to messages sent.
Flags	Attribute used to identify or track data.
Data	Information.
Last sent Src_instance	Last source instance identifier sent.
HELLO READ DB	Storage area for standby RP hello data. This field is blank on an active RP except when it is in recovery mode.

Hello Example on Standby RP

The following is sample output from the **show ip rsvp high-availability database hello** command on a standby RP:

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB

HELLO READ DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865
```

These fields are the same as those for the active RP described in Table 58 except they are now in the read database for the standby RP.

Link-Management Interfaces Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database link-management interfaces** command on an active RP:

```
Router# show ip rsvp high-availability database link-management interfaces
```

```
TE LINK WRITE DB
Flooding Protocol: ospf  IGP Area ID: 0  Link ID: 0 (GigabitEthernet3/2)
  Header:
    State: Checkpointed     Action: Add
    Seq #: 4                Flags: 0x0
  Data:
        Ifnumber: 5  Link Valid Flags: 0x193B
        Link Subnet Type: Broadcast
        Local Intfc ID: 0  Neighbor Intf ID: 0
        Link IP Address: 172.16.3.1
        Neighbor IGP System ID: 172.16.3.2  Neighbor IP Address: 10.0.0.0
        IGP Metric: 1  TE Metric: 1
        Physical Bandwidth: 1000000 kbits/sec
        Res. Global BW: 3000 kbits/sec
        Res. Sub BW: 0 kbits/sec
        Upstream::
                                 Global Pool   Sub Pool
                                 -----------   ----------
        Reservable Bandwidth[0]:           0            0 kbits/sec
        Reservable Bandwidth[1]:           0            0 kbits/sec
        Reservable Bandwidth[2]:           0            0 kbits/sec
        Reservable Bandwidth[3]:           0            0 kbits/sec
        Reservable Bandwidth[4]:           0            0 kbits/sec
        Reservable Bandwidth[5]:           0            0 kbits/sec
        Reservable Bandwidth[6]:           0            0 kbits/sec
        Reservable Bandwidth[7]:           0            0 kbits/sec
        Downstream::
                                 Global Pool   Sub Pool
                                 -----------   ----------
        Reservable Bandwidth[0]:        3000            0 kbits/sec
        Reservable Bandwidth[1]:        3000            0 kbits/sec
        Reservable Bandwidth[2]:        3000            0 kbits/sec
        Reservable Bandwidth[3]:        3000            0 kbits/sec
        Reservable Bandwidth[4]:        3000            0 kbits/sec
        Reservable Bandwidth[5]:        3000            0 kbits/sec
        Reservable Bandwidth[6]:        3000            0 kbits/sec
        Reservable Bandwidth[7]:        2900            0 kbits/sec
        Affinity Bits: 0x0
        Protection Type: Capability 0,  Working Priority 0
        Number of TLVs: 0
```

Table 59 describes the significant fields shown in the display.

Table 59 show ip rsvp high-availability database link-management interfaces—Active RP Field Descriptions

Field	Description
TE LINK WRITE DB	Storage area for active TE RP link data. This field is blank on a standby RP.
Flooding Protocol	Protocol that is flooding information for this area. ospf = Open Shortest Path First.
IGP Area ID	Interior Gateway Protocol (IGP) identifier for the area being flooded.
Link ID	Link identifier and interface for the area being flooded.
Header	Header information.

Table 59 show ip rsvp high-availability database link-management interfaces—Active RP Field Descriptions (continued)

Field	Description
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent, but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Numbers used by the active and standby RPs to synchronize message acks and nacks to messages sent.
Flags	Attribute used to identify or track data.
Data	Information.
Ifnumber	Interface number.
Link Valid Flags	Attributes used to identify or track links.
Link Subnet Type	Subnet type of the link. Values are as follows: • Broadcast—Data for multiple recipients. • Nonbroadcast Multiaccess—A network in which data is transmitted directly from one computer to another over a virtual circuit or across a switching fabric. • Point-to-Multipoint—Unidirectional connection in which a single source end system (known as a root node) connects to multiple destination end systems (known as leaves). • Point-to-Point—Unidirectional or bidirectional connection between two end systems. • Unknown subnet type—Subnet type not identified.
Local Intfc ID	Local interface identifier.
Neighbor Intf ID	Neighbor's interface identifier.
Link IP Address	IP address of the link.
Neighbor IGP System ID	Neighbor system identifier configured using IGP.
Neighbor IP Address	Neighbor's IP address.
IGP Metric	Metric value for the TE link configured using IGP.

Table 59 show ip rsvp high-availability database link-management interfaces—Active RP Field Descriptions (continued)

Field	Description
TE Metric	Metric value for the TE link configured using Multiprotocol Label Switching (MPLS) TE.
Physical Bandwidth	Link bandwidth capacity (in kilobits per second).
Res. Global BW	Amount of reservable global pool bandwidth (in kilobits per second) on this link.
Res. Sub BW	Amount of reservable subpool bandwidth (in kilobits per second) on this link.
Upstream	Header for the following section of bandwidth values.
Global Pool	Global pool bandwidth (in kilobits per second) on this link.
Sub Pool	Subpool bandwidth (in kilobits per second) on this link.
Reservable Bandwidth [1]	Amount of bandwidth (in kilobits per second) available for reservations in the global TE topology and subpools.
Downstream	Header for the following section of bandwidth values.
Affinity Bits	Link attributes required in tunnels.
Protection Type	LSPs protected by fast reroute (FRR). Capability = LSPs capable of using FRR. Working Priority = LSPs actually using FRR.
Number of TLVs	Number of type, length, values (TLVs).

The fields for a standby RP are the same as those described in Table 59 except they are now in the TE link read database instead of the TE link write database that is used by an active RP.

Link-Management System Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database link-management system** command on an active RP:

```
Router# show ip rsvp high-availability database link-management system

TE SYSTEM WRITE DB
Flooding Protocol: OSPF  IGP Area ID: 0
  Header:
    State: Checkpointed     Action: Modify
    Seq #: 4                Flags: 0x0
  Data:
    LM Flood Data::
      LSA Valid flags: 0x0  Node LSA flag: 0x0
      IGP System ID: 172.16.3.1  MPLS TE Router ID: 10.0.0.3
      Flooded links: 1  TLV length: 0 (bytes)
      Fragment id: 0


TE SYSTEM READ DB
```

Table 60 describes the significant fields shown in the display.

Table 60 show ip rsvp high-availability database link-management system—Active RP Field Descriptions

Field	Description
TE SYSTEM WRITE DB	Storage area for active TE RP system data. This field is blank on a standby RP.
Flooding Protocol	Protocol that is flooding information for this area. OSPF = Open Shortest Path First.
IGP Area ID	IGP identifier for the area being flooded.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent, but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Numbers used by the active and standby RPs to synchronize message acks and nacks to messages sent.
Flags	Attribute used to identify or track data.
Data	Information.
LM Flood Data	Link management (LM) flood data.
LSA Valid flags	Link-state advertisement (LSA) attributes.
Node LSA flag	LSA attributes used by a router.
IGP System ID	Identification (IP address) that IGP flooding uses in this area to identify this node.
MPLS TE Router ID	MPLS TE router identifier (IP address).
Flooded links	Number of flooded links.
TLV length	TLV length in bytes.
Fragment id	Fragment identifier for this link.
TE SYSTEM READ DB	Storage area for standby TE RP system data. This field is blank on a standby RP.

The fields for a standby RP are the same as those described in Table 60 except they are now in the TE system read database instead of the TE system write database that is used by an active RP.

LSP Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database lsp** command on an active RP:

```
Router# show ip rsvp high-availability database lsp

LSP WRITE DB
Tun ID: 10   LSP ID: 8
  Dest:   10.0.0.9
  Sender: 10.0.0.3     Ext. Tun ID: 10.0.0.3
  Header:
    State: Checkpointed     Action: Add
    Seq #: 3                Flags: 0x0
  Data:
    InLabel: -
    Out I/F: Gi3/2
    Next-Hop: 172.16.3.1
    OutLabel: 17

Loose hop info:
10.0.0.2 10.10.2.2 10.10.2.3 10.1.1.1

LSP READ DB
```

Table 61 describes the significant fields shown in the display.

Table 61 show ip rsvp high-availability database lsp—Active RP Field Descriptions

Field	Description
LSP WRITE DB	Storage area for active RP LSP data. This field is blank on a standby RP.
Tun ID	Tunnel identifier.
LSP ID	LSP identifier.
Dest	Tunnel destination IP address.
Sender	Tunnel sender IP address.
Ext. Tun ID	Extended tunnel identifier; usually set to 0 or the sender's IP address.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent, but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.

Table 61 show ip rsvp high-availability database lsp—Active RP Field Descriptions (continued)

Field	Description
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Numbers used by the active and standby RPs to synchronize message acks and nacks to messages sent.
Flags	Attribute used to identify or track data.
Data	Information.
InLabel	Incoming label identifier.
Out I/F	Outgoing interface.
Next-Hop	Next hop IP address.
OutLabel	Outgoing label identifier.
Loose hop info	Lists the loose hop expansions performed on the router, or specifies None.
LSP READ DB	Storage area for standby RP LSP data. This field is blank on an active RP.

The fields for a standby RP are the same as those described in Table 61 except they are now in the LSP read database instead of the LSP write database that is used by an active RP.

LSP-Head Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database lsp-head** command on an active RP:

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
 Tun ID: 10
 Header:
  State: Checkpointed   Action: Add
  Seq #: 3              Flags: 0x0
 Data:
    lsp_id: 8, bandwidth: 100, thead_flags: 0x1, popt: 1
    feature_flags: path protection active
    output_if_num: 5, output_nhop: 172.16.3.2
    RRR path setup info
     Destination: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf) flag:0x0
     IGP: ospf, IGP area: 0, Number of hops: 5, metric: 2
     Hop 0: 172.16.3.1, Id: 172.16.3.1 Router Node (ospf), flag:0x0
     Hop 1: 172.16.3.2, Id: 10.0.0.7 Router Node (ospf), flag:0x0
     Hop 2: 172.16.6.1, Id: 10.0.0.7 Router Node (ospf), flag:0x0
     Hop 3: 172.16.6.2, Id: 10.0.0.9 Router Node (ospf), flag:0x0
     Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf), flag:0x0

LSP_HEAD READ DB
```

Table 62 describes the significant fields shown in the display.

Table 62 show ip rsvp high-availability database lsp-head—Active RP Field Descriptions

Field	Description
LSP_HEAD WRITE DB	Storage area for active RP LSP-head data. This field is blank on a standby RP.
Tun ID	Tunnel identifier.
Header	Header information.
State	Status of an entry. Values are as follows: • Ack-Pending—Entries have been sent, but not acknowledged. • Checkpointed—Entries have been sent and acknowledged by the standby RP. • Send-Pending—Entries are waiting to be sent.
Action	Action taken. Values are as follows: • Add—Adding an item to the standby RP. • Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation. • Modify—Modifying an item on the standby RP. • Remove—Removing an item from the standby RP.
Seq #	Numbers used by the active and standby RPs to synchronize message acks and nacks to messages sent.
Flags	Attribute used to identify or track data.
Data	Information.
lsp_id	LSP identifier.
bandwidth	Bandwidth on the LSP (in kilobits per second).
thead_flags	Tunnel head attribute used to identify or track data.
popt	Parsing option number.
feature_flags	Indicates whether the LSP being used to forward traffic is the secondary LSP using the path protection path-option. Valid values are as follows: • none • path protection active
output_if_num	Output interface number.
output_nhop	Output next hop IP address.
RRR path setup info	Routing with Resource Reservation (RRR) path information.
Destination	Destination IP address.

Table 62 show ip rsvp high-availability database lsp-head—Active RP Field Descriptions

Field	Description
Id	IP address and protocol of the routing node. Values are the following: • isis = Intermediate System-to-Intermediate System • ospf = Open Shortest Path First
flag	Attribute used to track data.
IGP	Interior Gateway Protocol. ospf = Open Shortest Path First.
IGP area	IGP area identifier.
Number of hops	Number of connections or routers.
metric	Routing cost.
Hop	Hop's number and IP address.
Id	IP address and protocol of the routing node. Values are the following: • isis = Intermediate System-to-Intermediate System • ospf = Open Shortest Path First
flag	Attribute used to track data.
LSP_HEAD READ DB	Storage area for standby RP LSP-head data. This field is blank on an active RP.

The fields for a standby RP are the same as those described in Table 62 except they are now in the LSP_head read database instead of the LSP_head write database that is used by an active RP.

Summary Example on an Active RP

The following is sample output from the **show ip rsvp high-availability database summary** command on an active RP:

```
Router# show ip rsvp high-availability database summary

Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:    10
  Total       :    10

Read DB:
  Total       :     0
```

Table 63 describes the significant fields shown in the display.

Table 63 show ip rsvp high-availability database summary—Active RP Field Descriptions

Field	Description
Write DB	Storage area for active RP summary data. This field is blank on a standby RP.
Send-Pending	Entries are waiting to be sent.

Table 63 show ip rsvp high-availability database summary—Active RP Field Descriptions

Field	Description
Ack-Pending	Entries have been sent, but are waiting to be acknowledged.
Checkpointed	Entries have been sent and acknowledged.
Total	Total number of entries in the write database.
Total	Total number of entries in the read database.

Summary Example on a Standby RP

The following is sample output from the **show ip rsvp high-availability database summary** command on a standby RP:

```
Router# show ip rsvp high-availability database summary

Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:     0
  Total       :     0

Read DB:
  Total       :    10
```

Table 64 describes the significant fields shown in the display.

Table 64 show ip rsvp high-availability database summary—Standby RP Field Descriptions

Field	Description
Write DB	Storage area for active RP summary data.
Send-Pending	Entries are waiting to be sent.
Ack-Pending	Entries have been sent, but are waiting to be acknowledged.
Checkpointed	Entries have been sent and acknowledged.
Total	Total number of entries in the write DB.
Total	Total number of entries in the read DB.

Related Commands

Command	Description
show ip rsvp high-availability counters	Displays all RSVP HA counters that are being maintained by an RP.
show ip rsvp high-availability summary	Displays summary information for an RSVP HA RP.

show ip rsvp host

To display specific information for a Resource Reservation Protocol (RSVP) host, use the **show ip rsvp host** command in user EXEC or privileged EXEC mode.

show ip rsvp host {**senders** | **receivers**} [*group-name* | *group-address*]

Syntax Description

senders	RSVP-related sender information currently in the database.
receivers	RSVP-related receiver information currently in the database.
group-name	(Optional) Hostname of the source or destination.
group-address	(Optional) IP address of the source or destination.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(6)T	The command output was modified to display RSVP identity information when configured.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show ip rsvp host** command to display static RSVP senders and receivers. If a router has any local host receivers or senders that have RSVP identities configured, the application IDs that they use are also displayed.

Examples

In the following example from the **show ip rsvp host senders** command, no RSVP identities are configured for the local sender:

```
Router# show ip rsvp host senders

To            From          Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                            10K
  Mode(s): Host CLI
```

Table 65 describes the significant fields shown in the display.

Table 65 show ip rsvp host senders (No RSVP Identities Configured) Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. IP protocol such as TCP or UDP.

Table 65 show ip rsvp host senders (No RSVP Identities Configured) Field Descriptions

Field	Description
DPort	Destination port number. Code 1 indicates IP protocol such as TCP or UDP.
Sport	Source port number. Code 1 indicates IP protocol such as TCP or UDP.
Prev Hop	IP address of the previous hop. Blank means no previous hop.
I/F	Interface of the previous hop.
BPS	Reservation rate, in bits per second (bps).
Mode(s)	Any of the following strings: • Host—The router is acting as the host system or RSVP endpoint for this reservation. • LSP-Tunnel—The reservation is for a Traffic Engineering (TE) tunnel. • MIB—The reservation was created via an SNMP SET directive from a remote management station. • CLI—The reservation was created via a local RSVP CLI command. • Host CLI—A combination of the host and CLI strings meaning that the static sender being displayed was created by the **ip rsvp sender-host** CLI command.

In the following example from the **show ip rsvp host senders** command, an RSVP identity is configured for the local sender and more information displays:

```
Router# show ip rsvp host senders

To            From          Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                            10K
  Mode(s): Host CLI
  Identity: voice100
    Locator: GUID=www.cisco.com,APP=voice,VER=100.0
    ID Type: Application
```

Table 66 describes the significant fields shown in the display.

Table 66 show ip rsvp host senders (RSVP Identity Configured) Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. IP protocol such as TCP or UDP.
DPort	Destination port number. Code 1 indicates IP protocol such as TCP or UDP.
Sport	Source port number. Code 1 indicates IP protocol such as TCP or UDP.
Prev Hop	IP address of the previous hop. Blank means no previous hop.

Table 66 show ip rsvp host senders (RSVP Identity Configured) Field Descriptions (continued)

Field	Description
I/F	Interface of the previous hop.
BPS	Reservation rate in bits per second (bps).
Mode(s)	Any of the following strings: • Host—The router is acting as the host system or RSVP endpoint for this reservation. • LSP-Tunnel—The reservation is for a Traffic Engineering (TE) tunnel. • MIB—The reservation was created via an SNMP SET directive from a remote management station. • CLI—The reservation was created via a local RSVP CLI command. • Host CLI—A combination of the host and CLI strings meaning that the static sender being displayed was created by the **ip rsvp sender-host** CLI command.
Identity	The alias string for the RSVP application ID.
Locator	The application ID that is being signaled in the RSVP PATH message for this statically-configured sender.
ID Type	Types of identities. RSVP defines two types: application IDs (Application) and user IDs (User). Cisco IOS software currently supports Application only.

Related Commands

Command	Description
ip rsvp sender-host	Enables a router to simulate a host generating an RSVP PATH message.

show ip rsvp interface detail

To display the interface configuration for Hello, use the **show ip rsvp interface detail** command in privileged EXEC mode.

show ip rsvp interface detail [*interface*]

Syntax Description

interface	(Optional) Interface for which you want to show the Hello configuration.

Command Default

The interface configuration for Hello is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following is sample output from the **show ip rsvp interface detail** command:

```
Router# show ip rsvp interface detail GigabitEthernet 9/47

Gi9/47:
 RSVP: Enabled
 Interface State: Up
 Bandwidth:
  Curr allocated: 0 bits/sec
  Max. allowed (total): 0 bits/sec
  Max. allowed (per flow): 0 bits/sec
  Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
  Set aside by policy (total): 0 bits/sec
 Signalling:
  DSCP value used in RSVP msgs: 0x3F
  Number of refresh intervals to enforce blockade state: 4
 Authentication: disabled
  Key chain: <none>
  Type:  md5
  Window size: 1
  Challenge:  disabled
 FRR Extension:
  Backup Path: Configured (or "Not Configured")
 BFD Extension:
  State: Disabled
  Interval: Not Configured
 RSVP Hello Extension:
  State: Disabled
```

```
Refresh Interval: FRR: 200  , Reroute: 2000
Missed Acks:      FRR: 4    , Reroute: 4
DSCP in HELLOs:   FRR: 0x30 , Reroute: 0x30
```

Table 67 describes the significant fields shown in the display.

Table 67 show ip rsvp interface detail Field Descriptions

Field	Description
RSVP	Status of the Resource Reservation Protocol (RSVP) protocol (Enabled or Disabled).
Interface State	Status of the interface (Up or Down).
Curr allocated	Amount of bandwidth (in bits per second [bps]) currently allocated.
Max. allowed (total)	Total maximum amount of bandwidth (in bps) allowed.
Max. allowed (per flow)	Maximum amount of bandwidth (in bps) allowed per flow.
Max. allowed for LSP tunnels using sub-pools	Maximum amount of bandwidth permitted for label-switched path (LSP) tunnels that obtain their bandwidth from subpools.
DSCP value used in RSVP msgs	The differentiated services code point (DSCP) value that is in RSVP messages.
BFD Extension State	State (Enabled or Disabled) of BFD extension.
RSVP Hello Extension State	State (Enabled or Disabled) of Hello extension.
Missed Acks	Number of sequential acknowledgments that the node did not receive.
DSCP in HELLOs	The DSCP value that is in hello messages.

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the hello message sent out from an interface.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.

show ip traffic-engineering

To display information about the traffic engineering configuration and metric information associated with it, use the **show ip traffic-engineering** command in privileged EXEC mode.

show ip traffic-engineering [**metrics** [**detail**]]

Syntax Description

metrics	(Optional) Displays metric information associated with traffic engineering.
detail	(Optional) Displays information in long form.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The goal of the loop prevention algorithm is that traffic should not be sent down the tunnel if there is a possibility that, after leaving the tunnel, steady state routing will route the traffic back to the head of the tunnel.

The strategy of the loop prevention algorithm is to compare the Layer 3 routing distance to the egress from the tunnel tailend and tunnel headend. The loop check passes only if the tunnel tail is closer to the egress than the tunnel head is.

The loop prevention algorithm allows you to use the tunnel for a route if one the following cases applies:

- Given that the two ends of the tunnel are routing to the egress using the same dynamic protocol in the same area, the Layer 3 routing distance from the tailend to the egress is less than the Layer 3 routing distance from the headend to the egress.
- The route to the egress is directly connected at the tunnel tailend router, but not at the tunnel headend router.
- The egress is unreachable from the tunnel headend router, but is reachable from the tunnel tailend router.

The loop prevention algorithm prevents you from using the tunnel for a given egress in all other cases, in particular, the following cases:

- The routers at the ends of the tunnel get their route to the egress from different dynamic routing protocols.
- The routing protocols at the two ends of the tunnel route to the egress through different areas.
- The two ends each use a static route to the egress.

- The tunnel headend router's route to the egress is a connected route.
- The egress is unreachable from the tunnel tailend router.

Devices request metrics via an LDP adjacency. The display output shows detailed metric information.

The metric information includes a metric type (shown as routing_protocol/routing_protocol_subtype) and a metric value.

The routing protocol is as follows:

- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Connected
- Static
- Other (some other routing protocol)

The routing protocol subtype is specific to each routing protocol.

Examples

The following is sample output from the **show ip traffic-engineering metrics detail** command:

```
Router# show ip traffic-engineering metrics detail

Metrics requested BY this device
 Prefix 43.0.0.1/32
  TDP id 2.2.2.2:0, metric: connected/0
    type request, flags metric-received, rev 6, refcnt 1
  TDP id 4.4.4.4:0, metric: ospf-300/2
    type request, flags metric-received, rev 7, refcnt 1
 Prefix 44.0.0.0/8
  TDP id 18.18.18.18:0, metric: connected/0
    type request, flags metric-received, rev 1, refcnt 1
Metrics requested FROM this device
 Prefix 36.0.0.0/8
  TDP id 18.18.18.18:0, metric: connected/0
    type advertise, flags none, rev 1, refcnt 1
```

Table 68 describes the significant fields shown in the display.

Table 68 show ip traffic-engineering metrics detail Field Descriptions

Field	Description
Prefix	Destination network and mask.
TDP id	The LDP identifier of the LDP peer device at the other end of the tunnel. The LDP peer device advertises these metrics to this neighbor.
metric	The routing protocol and metric within that protocol for the prefix in question.
type	For metrics being requested by this device, the type is either "request" or "release." For metrics being requested from this device, the type is "advertise."

Table 68 show ip traffic-engineering metrics detail Field Descriptions (continued)

flags	For metrics being requested by this device, "metric-received" indicates that the other end has responded with a metric value. For metrics being requested from this device, response-pending indicates that the metric value has not yet been sent to the requester.
rev	An internal identifier for the metric request or advertisement. The rev number is assigned when the request/advertisement is created. The rev number is updated if the local information for the metric changes.
refcnt	For a metric of type request, the number of traffic engineering routes interested in this metric value. Otherwise, refcnt is 1.

Related Commands

Command	Description
traffic-engineering filter	Specifies a filter with a given number and properties.
traffic-engineering route	Configures a route for a specified filter, through a specified tunnel.

show ip traffic-engineering configuration

To display information about configured traffic engineering filters and routes, use the **show ip traffic-engineering configuration** command in privileged EXEC mode.

show ip traffic-engineering configuration [*interface*] [*filter-number*] [**detail**]

Syntax Description

interface	(Optional) Specifies an interface for which to display traffic engineering information.
filter-number	(Optional) A decimal value representing the number of the filter to display.
detail	(Optional) Displays command output in long form.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The sample output can show all filters or can be limited by interface, filter number, or both.

Examples

The following is sample output from the **show ip traffic-engineering configuration detail** command:

```
Router# show ip traffic-engineering configuration detail

Traffic Engineering Configuration
    Filter 5: egress 44.0.0.0/8, local metric: ospf-0/1
        Tunnel5 route installed
          interface up, preference 1
          loop check on, passing, remote metric: connected/0
    Filter 6: egress 43.0.0.1/32, local metric: ospf-300/3
        Tunnel7 route installed
          interface up, preference 50
          loop check on, passing, remote metric: ospf-300/2
        Tunnel6 route not installed
          interface up, preference 75
          loop check on, passing, remote metric: connected/0
```

Table 69 describes the significant fields shown in the display.

Table 69 show ip traffic-engineering configuration detail Field Descriptions

Field	Description
Filter	The configured filter identifier for the traffic engineering route.
egress	The prefix/mask configured with the filter local metric.
local metric	The routing protocol and metric value of the local LSR for the egress prefix/mask.
Tunnel5	The tunnel for the traffic engineering route.
route installed/not installed	Indicates whether the route is installed in the forwarding tables (typically CEF and label interface up/down).
interface	Indicates whether the tunnel interface for the traffic engineering route is up or down. The traffic engineering route is not installed if the tunnel interface is down.
preference	The configured administrative preference for the traffic engineering route.
loop check	Indicates whether the loop check has been configured on or off.
passing/failing	If the loop check is configured on, indicates whether the check is passing. The traffic engineering route is not installed if the loop check is configured on and is failing.
remote metric	The routing protocol and the metric within that protocol for the prefix in question, as seen by the LSR that is advertising the metric. As part of the loop check, a comparison is made between the remote metric and the local metric.

Related Commands

Command	Description
show ip traffic-engineering routes	Displays information about the requested filters configured for traffic engineering.

show ip traffic-engineering routes

To display information about the requested filters configured for traffic engineering, use the **show ip traffic-engineering routes** command in privileged EXEC mode.

show ip traffic-engineering routes [*filter-number*] [**detail**]

Syntax Description

filter-number	(Optional) A decimal value representing the number of the filter to display.
detail	(Optional) Display of command output in long form.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Requests can be limited to a specific filter.

Examples

The following is sample output from the **show ip traffic-engineering routes** command:

```
Router# show ip traffic-engineering routes

Installed traffic engineering routes:
Codes: T - traffic engineered route
T    43.0.0.1/32 (not override of routing table entry)
                is directly connected, 00:06:35, Tunnel7
T    44.0.0.0/8 (override of routing table entry)
              is directly connected, 01:12:39, Tunnel5
```

Table 70 describes the significant fields shown in the display.

Table 70 show ip traffic-engineering routes Field Descriptions

Field	Description
T	Traffic engineering route.
43.0.0.1/32 (not override of routing table entry) is directly connected	Prefix/mask being routed. The routing table does not contain an entry for this prefix/mask.
00:06:35	The time since the route was installed (hours:minutes:seconds).
Tunnel7	The LSP tunnel for the route.

Related Commands

Command	Description
show ip traffic-engineering configuration	Displays information about configured traffic engineering filters and routes.

show ip vrf

To display the set of defined Virtual Private Network (VPN) routing and forwarding (VRF) instances and associated interfaces, use the **show ip vrf** command in privileged EXEC mode.

show ip vrf [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*] [*output-modifiers*]

Syntax Description

brief	(Optional) Displays concise information on the VRFs and associated interfaces.
detail	(Optional) Displays detailed information on the VRFs and associated interfaces.
interfaces	(Optional) Displays detailed information about all interfaces bound to a particular VRF or any VRF.
id	(Optional) Displays the VPN IDs that are configured in a PE router for different VPNs.
vrf-name	(Optional) Name assigned to a VRF.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

Defaults

When no keywords or arguments are specified, the command shows concise information about all configured VRFs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(17)ST	This command was modified to include the **id** keyword, and VPN ID information was added to the output of the **show ip vrf detail** command.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(6)	This command was integrated into Cisco IOS Release 12.3(6). The command shows the downstream VRF for each associated Virtual access interface (VAI).
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) VRF support was added.
12.2(15)T	EIGRP VRF support was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP VRF support was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display information about VRFs. Two levels of detail are available:

- The **brief** keyword (or no keyword) displays concise information.
- The **detail** keyword displays all information.

To display information about all interfaces bound to a particular VRF, or to any VRF, use the **interfaces** keyword. To display information about VPN IDs assigned to a PE router, use the **id** keyword.

Examples

The following example displays information about all the VRFs configured on the router, including the downstream VRF for each associated VAI. The lines that are highlighted (for documentation purposes only) indicate the downstream VRF.

```
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
```

Table 71 describes the significant fields shown in the display.

Table 71 show ip vrf Field Descriptions

Field	Description
Name	Specifies the VRF name.
Default RD	Specifies the default route distinguisher.
Interface	Specifies the network interface.

The following example displays detailed information about all of the VRFs configured on the router, including all of the VAIs associated with each VRF:

```
Router# show ip vrf detail

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
```

Table 72 describes the significant fields shown in the display.

Table 72 show ip vrf detail Field Descriptions

Field	Description
VPNID	Specifies the VPN ID assigned to the VRF.
Interfaces	Specifies the network interfaces.
Virtual-Access*n* [D]	Specifies the downstream VRF.
Export	Specifies VPN route-target export communities.
Import	Specifies VPN route-target import communities.

The following example shows the interfaces bound to a particular VRF:

```
Router# show ip vrf interfaces

InterfaceIP-AddressVRFProtocol
Ethernet210.22.0.33vrf1up
Ethernet410.77.0.33hubup
Router#
```

Table 73 describes the significant fields shown in the display.

Table 73 show ip vrf interfaces Field Descriptions

Field	Description
Interface	Specifies the network interfaces for a VRF.
IP-Address	Specifies the IP address of a VRF interface.
VRF	Specifies the VRF name.
Protocol	Displays the state of the protocol (up or down) for each VRF interface.

The following is sample output that shows all the VPN IDs that are configured in the router and their associated VRF names and VRF route distinguishers (RDs):

```
Router# show ip vrf id

VPN Id          Name                            RD
2:3             vpn2                            <not set>
A1:3F6C         vpn1                            100:1
```

Table 74 describes the significant fields shown in the display.

Table 74 show ip vrf id Field Descriptions

Field	Description
VPN Id	Specifies the VPN ID assigned to the VRF.
Name	Specifies the VRF name.
RD	Specifies the route distinguisher.

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
ip vrf forwarding (interface configuration)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF.
route-target	Creates a route-target extended community for a VRF.
vpn id	Assigns a VPN ID to a VRF.

show isis database verbose

To display additional information about the Intermediate System-to-Intermediate System (IS-IS) database, use the **show isis database verbose** command in user EXEC or privileged EXEC mode.

show isis database verbose

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show isis database verbose** command:

```
Router# show isis database verbose

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
dtp-5.00-00         * 0x000000E6   0xC9BB        1042              0/0/0
  Area Address:49.0001
  NLPID:       0xCC
  Hostname:dtp-5
  Router ID:   10.5.5.5
  IP Address:  172.16.39.5
  Metric:10         IP 172.16.39.0/24
dtp-5.00-01         * 0x000000E7   0xAB36        1065              0/0/0
  Metric:10         IS-Extended dtp-5.01
    Affinity:0x00000000
    Interface IP Address:172.21.39.5
    Physical BW:10000000 bits/sec
    Reservable BW:1166000 bits/sec
    BW Unreserved[0]: 1166000 bits/sec, BW Unreserved[1]: 1166000 bits/sec
    BW Unreserved[2]: 1166000 bits/sec, BW Unreserved[3]: 1166000 bits/sec
    BW Unreserved[4]: 1166000 bits/sec, BW Unreserved[5]: 1166000 bits/sec
    BW Unreserved[6]: 1166000 bits/sec, BW Unreserved[7]: 1153000 bits/sec
  Metric:0          ES dtp-5
```

Table 75 describes the significant fields shown in the display.

Table 75 show isis database verbose Field Descriptions

Field	Description
LSPID	Link-state packet (LSP) identifier. The first six octets form the System ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. This is similar to a router LSA in Open Shortest Path First (OSPF); the LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP that describes all systems attached to that LAN. The last octet is the LSP number. If all the data cannot fit into a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the system issuing this command originated the LSP.
LSP Seq Num	LSP sequence number that allows other systems to determine if they received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time that the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from all routers' link-state databases (LSDBs). The value indicates how long the purged LSP will stay in the LSDB before it is completely removed.
ATT	Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1 routers use the Attach bit to find the closest Level 2 router. They install a default route to the closest Level 2 router.
P	P bit. This bit detects if the IS can repair area partitions. Cisco and other vendors do not support area partition repair.
OL	Overload bit. This bit determines if the IS is congested. If the overload bit is set, other routers do not use this system as a transit router when they calculate routes. Only packets for destinations directly connected to the overloaded router are sent to this router.
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
NLPID	Network Layer Protocol identifier.
Hostname	Hostname of the node.
Router ID	Traffic engineering router identifier for the node.
IP Address	IPv4 address for the interface.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a connectionless network service [CLNS] prefix).
Affinity	Link attribute flags that are being flooded.

Table 75 show isis database verbose Field Descriptions (continued)

Field	Description
Physical BW	Link bandwidth capacity (in bits per second).
Reservable BW	Amount of reservable bandwidth on this link.
BW Unreserved	Amount of bandwidth that is available for reservation.

The following example includes a route tag:

```
Router# show isis database verbose

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num    LSP Checksum    LSP Holdtime    ATT/P/OL
dasher.00-00          0x000000F8     0xE57B          518             1/0/0
  Area Address: 49.0002
  NSPID:        0xCC
  Hostname: dasher
  IP Address: 10.3.0.1
  Metric: 10     IP 172.16.170.0/24
  Metric: 10     IP 10.0.3.0/24
  Metric: 10     IP 10.0.3.3/30
  Metric: 10     IS-Extended dasher.02172.19.170.0/24
  Metric: 20     IP-Interarea 10.1.1.1/32
    Route Admin Tag: 60
  Metric: 20     IP-Interarea 192.168.0.6/32
    Route Admin Tag: 50
```

Related Commands

Command	Description
show isis mpls traffic-eng adjacency-log	Displays a log of 20 entries of MPLS traffic engineering IS-IS adjacency changes.
show isis mpls traffic-eng advertisements	Displays the last flooded record from MPLS traffic engineering.
show isis mpls traffic-eng tunnel	Displays information about tunnels considered in the IS-IS next hop calculation.

show isis mpls ldp

To display synchronization and autoconfiguration information about interfaces belonging to Intermediate System-to-Intermediate System (IS-IS) processes, use the **show isis mpls ldp** command in privileged EXEC mode.

show isis [*process-tag*] **mpls ldp** [**interface** *interface*]

Syntax Description

process-tag	(Optional) Process ID. Displays information only for the specified routing process.
interface *interface*	(Optional) Defines the interface for which Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization and LDP autoconfiguration information will be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modifications
12.0(32)SY	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command shows Multiprotocol Label Switching (MPLS) LDP synchronization and autoconfiguration information for interfaces that are running IS-IS processes. If you do not specify a keyword or argument, information appears for each interface that is configured for MPLS LDP synchronization and autoconfiguration. MPLS LDP synchronization and autoconfiguration for IS-IS is supported only in Cisco IOS Release 12.0(32)SY.

Examples

In the following example, interface POS0/2 is running IS-IS. Autoconfiguration is enabled. Synchronization is configured.

```
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: YES
   Achieved: YES
   IGP Delay: NO
   Holddown time: Infinite
   State: SYNC achieved
```

This command returns information for interfaces that are configured for IS-IS, which are indicated by the message “ISIS is UP” on the interface.

Table 76 describes the significant fields shown in the display.

Table 76 show isis mpls ldp Field Descriptions

Field	Description
AUTOCONFIG Information	LDP enabled—Indicates whether LDP autoconfiguration is enabled on this interface. Value is YES or NO.
SYNC Information	Provides synchronization information. • Required—Indicates whether synchronization is required on the interface. • Achieved—Indicates whether synchronization was achieved with LDP. If IS-IS was configured on an interface but synchronization is not achieved, the Achieved field indicates NO. The Required field still indicates YES. • IGP Delay—Indicates whether the IS-IS process must wait for synchronization with LDP before bringing up the interface adjacency. • Holddown time—Valid values are Finite or Infinite. The finite value is equal to the hold-down delay that you configured using the **mpls ldp igp sync holddown** command. If this field indicates Infinite, hold-down time was not configured. Therefore, IS-IS waits until synchronization is achieved before bringing adjacency UP. The Holddown time field is significant only if the IGP Delay field indicates YES. • State—Indicates information about the state of synchronization on the interface. If synchronization is achieved, the output shows the following: – SYNC achieved—Synchronization was required and has been achieved. If synchronization is not achieved, the output shows one of the following: – Holding down until SYNC—No hold-down timer was configured, so IS-IS continues to hold down adjacency until synchronization is achieved. – Holding down with timer—A hold-down timer was configured and IS-IS is holding down adjacency until the timer, indicated in the IGP Delay field, expires. – Maximum metric in effect—Although synchronization was not achieved, the IGP brought up adjacency with the maximum metric.

Related Commands

Command	Description
mpls ldp autoconfig	Globally enables LDP autoconfiguration on all interfaces that belong to an OSPF or IS-IS process.
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.

show isis mpls traffic-eng adjacency-log

To display a log of 20 entries of Multiprotocol Label Switching (MPLS) traffic engineering Intermediate System-to-Intermediate System (IS-IS) adjacency changes, use the **show isis mpls traffic-eng adjacency-log** command in user EXEC or privileged EXEC mode.

show isis mpls traffic-eng adjacency-log

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show isis mpls traffic-eng adjacency-log** command:

```
Router# show isis mpls traffic-eng adjacency-log

IS-IS RRR log
When      Neighbor ID        IP Address       Interface Status Level
04:52:52  0000.0024.0004.02  0.0.0.0          Et0/2     Up     level-1
04:52:50  0000.0026.0001.00  172.16.1.2        PO1/0/0   Up     level-1
04:52:37  0000.0024.0004.02  10.0.0.0          Et0/2     Up     level-1
```

Table 77 describes the significant fields shown in the display.

Table 77 show isis mpls traffic-eng adjacency-log Field Descriptions

Field	Description
When	Amount of time since the entry was recorded in the log.
Neighbor ID	Identification value of the neighbor.
IP Address	Neighbor IPv4 address.
Interface	Interface from which a neighbor is learned.
Status	Up (active) or Down (disconnected).
Level	Routing level.

Related Commands

Command	Description
show isis mpls traffic-eng advertisements	Displays the last flooded record from MPLS traffic engineering.

show isis mpls traffic-eng advertisements

To display the last flooded record from Multiprotocol Label Switching (MPLS) traffic engineering, use the **show isis mpls traffic-eng advertisements** command in user EXEC or privileged EXEC mode.

show isis mpls traffic-eng advertisements

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show isis mpls traffic-eng advertisements** command:

```
Router# show isis mpls traffic-eng advertisements

System ID:dtp-5.00
  Router ID:10.5.5.5
  Link Count:1
    Link[1]
      Neighbor System ID:dtp-5.01 (broadcast link)
      Interface IP address:172.21.39.5
      Neighbor IP Address:0.0.0.0
      Admin. Weight:10
      Physical BW:10000000 bits/sec
      Reservable BW:1166000 bits/sec
      BW unreserved[0]:1166000 bits/sec, BW unreserved[1]:1166000 bits/sec
      BW unreserved[2]:1166000 bits/sec, BW unreserved[3]:1166000 bits/sec
      BW unreserved[
4]:1166000 bits/sec, BW unreserved[5]:1166000 bits/sec
      BW unreserved[6]:1166000 bits/sec, BW unreserved[7]:1153000 bits/sec
      Affinity Bits:0x00000000
```

Table 78 describes the significant fields shown in the display.

Table 78 show isis mpls traffic-eng advertisements Field Descriptions

Field	Description
System ID	Identification value for the local system in the area.
Router ID	MPLS traffic engineering router ID.
Link Count	Number of links that MPLS traffic engineering advertised.
Neighbor System ID	Identification value for the remote system in an area.
Interface IP address	IPv4 address of the interface.
Neighbor IP Address	IPv4 address of the neighbor.
Admin. Weight	Administrative weight associated with this link.
Physical BW	Link bandwidth capacity (in bits per second).
Reservable BW	Amount of reservable bandwidth on this link.
BW unreserved	Amount of bandwidth that is available for reservation.
Affinity Bits	Link attribute flags being flooded.

Related Commands

Command	Description
show isis mpls traffic-eng adjacency-log	Displays a log of 20 entries of MPLS traffic engineering IS-IS adjacency changes.

show isis mpls traffic-eng tunnel

To display information about tunnels considered in the Intermediate System-to-Intermediate System (IS-IS) next hop calculation, use the **show isis mpls traffic-eng tunnel** command in privileged EXEC mode.

show isis mpls traffic-eng tunnel

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show isis mpls traffic-eng tunnel** command:

```
Router# show isis mpls traffic-eng tunnel

Station Id          Tunnel Name   Bandwidth    Nexthop       Metric   Mode
kangpa-router1.00   Tunnel1022    3333         10.2.2.2       -3       Relative
                    Tunnel1021    10000        10.2.2.2       11       Absolute
tomklong-route.00   Tunnel1031    10000        172.17.3.3       -1       Relative
                    Tunnel1032    10000        172.17.3.3
```

Table 79 describes the significant fields shown in the display.

Table 79 show isis mpls traffic-eng tunnel Field Descriptions

Field	Description
Station Id	Name or system ID of the MPLS traffic engineering tailend router.
Tunnel Name	Name of the MPLS traffic engineering tunnel interface.
Bandwidth	MPLS traffic engineering specified bandwidth of the tunnel.
Nexthop	MPLS traffic engineering destination IP address of the tunnel.
Metric	MPLS traffic engineering metric of the tunnel.
Mode	MPLS traffic engineering metric mode of the tunnel. It can be relative or absolute.

Related Commands

Command	Description
show mpls traffic-eng autoroute	Displays tunnels that are announced to IGP, including interface, destination, and bandwidth.

show issu clients

To display a list of the current In Service Software Upgrade (ISSU) clients—that is, the network applications and protocols supported by ISSU—use the **show issu clients** command in user EXEC or privileged EXEC mode.

show issu clients

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command lists all ISSU clients currently operating in the network, along with their Client ID numbers and the number of entities each client contains.

You should enter this command before you enter the **issu runversion** command, because if a client (application or protocol) that needs to continue operating in the network does not appear in the displayed list, you will know not to continue the software upgrade (because proceeding further with ISSU would then halt the operation of that application or protocol).

Examples

The following example shows a client list displayed by entering this command:

```
Router# show issu clients

Client_ID = 2,  Client_Name = ISSU Proto client,  Entity_Count = 1
Client_ID = 3,  Client_Name = ISSU RF,  Entity_Count = 1
Client_ID = 4,  Client_Name = ISSU CF client,  Entity_Count = 1
Client_ID = 5,  Client_Name = ISSU Network RF client,  Entity_Count = 1
Client_ID = 7,  Client_Name = ISSU CONFIG SYNC,  Entity_Count = 1
Client_ID = 8,  Client_Name = ISSU ifIndex sync,  Entity_Count = 1
Client_ID = 9,  Client_Name = ISSU IPC client,  Entity_Count = 1
Client_ID = 10,  Client_Name = ISSU IPC Server client,  Entity_Count = 1
Client_ID = 11,  Client_Name = ISSU Red Mode Client,  Entity_Count = 1
Client_ID = 12,  Client_Name = ISSU EHSA services client,  Entity_Count = 1
Client_ID = 100,  Client_Name = ISSU rfs client,  Entity_Count = 1
Client_ID = 110,  Client_Name = ISSU ifs client,  Entity_Count = 1
Client_ID = 1001,  Client_Name = OC3POS-6,  Entity_Count = 4
Client_ID = 1002,  Client_Name = C10K ATM,  Entity_Count = 1
Client_ID = 1003,  Client_Name = C10K CHSTM1,  Entity_Count = 1
Client_ID = 1004,  Client_Name = C10K CT3,  Entity_Count = 1
Client_ID = 1005,  Client_Name = C10K GE,  Entity_Count = 1
Client_ID = 1006,  Client_Name = C10K ET,  Entity_Count = 1
Client_ID = 1007,  Client_Name = C10K CHE1T1,  Entity_Count = 1
```

```
Client_ID = 1009,  Client_Name = C10K MFE,  Entity_Count = 1
Client_ID = 1010,  Client_Name = C10K APS,  Entity_Count = 1
Client_ID = 1013,  Client_Name = C10K CARD OIR,  Entity_Count = 1
Client_ID = 2002,  Client_Name = CEF Push ISSU client,  Entity_Count = 1
Client_ID = 2003,  Client_Name = ISSU XDR client,  Entity_Count = 1
Client_ID = 2004,  Client_Name = ISSU SNMP client,  Entity_Count = 1
Client_ID = 2005,  Client_Name = ISSU HDLC Client,  Entity_Count = 1
Client_ID = 2006,  Client_Name = ISSU QoS client,  Entity_Count = 1
Client_ID = 2007,  Client_Name = ISSU LSD Label Mgr HA Client,  Entity_Count = 1
Client_ID = 2008,  Client_Name = ISSU Tableid Client,  Entity_Count = 1
Client_ID = 2009,  Client_Name = ISSU MPLS VPN Client,  Entity_Count = 1
Client_ID = 2010,  Client_Name = ARP HA,  Entity_Count = 1
Client_ID = 2011,  Client_Name = ISSU LDP Client,  Entity_Count = 1
Client_ID = 2012,  Client_Name = ISSU HSRP Client,  Entity_Count = 1
Client_ID = 2013,  Client_Name = ISSU ATM Client,  Entity_Count = 1
Client_ID = 2014,  Client_Name = ISSU FR Client,  Entity_Count = 1
Client_ID = 2015,  Client_Name = ISSU REDSSOC client,  Entity_Count = 1
Client_ID = 2019,  Client_Name = ISSU TCP client,  Entity_Count = 1
Client_ID = 2020,  Client_Name = ISSU BGP client,  Entity_Count = 1
Client_ID = 2021,  Client_Name = XDR Int Priority ISSU client,  Entity_Count = 1
Client_ID = 2022,  Client_Name = XDR Proc Priority ISSU client,  Entity_Count = 1
Client_ID = 2023,  Client_Name = FIB HWIDB ISSU client,  Entity_Count = 1
Client_ID = 2024,  Client_Name = FIB IDB ISSU client,  Entity_Count = 1
Client_ID = 2025,  Client_Name = FIB HW subblock ISSU client,  Entity_Count = 1
Client_ID = 2026,  Client_Name = FIB SW subblock ISSU client,  Entity_Count = 1
Client_ID = 2027,  Client_Name = Adjacency ISSU client,  Entity_Count = 1
Client_ID = 2028,  Client_Name = FIB IPV4 ISSU client,  Entity_Count = 1
Client_ID = 2030,  Client_Name = MFI Pull ISSU client,  Entity_Count = 1
Client_ID = 2031,  Client_Name = MFI Push ISSU client,  Entity_Count = 1
Client_ID = 2051,  Client_Name = ISSU CCM Client,  Entity_Count = 1
Client_ID = 2052,  Client_Name = ISSU PPP SIP CCM Client,  Entity_Count = 1
Client_ID = 2054,  Client_Name = ISSU process client,  Entity_Count = 1

Base Clients:
 Client_Name = ISSU Proto client
 Client_Name = ISSU RF
 Client_Name = ISSU CF client
 Client_Name = ISSU Network RF client
 Client_Name = ISSU CONFIG SYNC
 Client_Name = ISSU ifIndex sync
 Client_Name = ISSU IPC client
 Client_Name = ISSU IPC Server client
 Client_Name = ISSU Red Mode Client
 Client_Name = ISSU EHSA services client
```

Table 80 describes the significant fields shown in the display.

Table 80 show issu clients Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for that client.
Client_Name	A character string describing the client. "Base Clients" are a subset, which includes: • Inter-Process Communications (IPC) • Redundancy Framework (RF) • Checkpoint Facility (CF) • Cisco Express Forwarding • Network RF (for IDB stateful switchover) • EHSA Services (including ifIndex) • Configuration Synchronization.
Entity_Count	The number of entities within this client. An entity is a logical group of sessions with some common attributes.

Related Commands

Command	Description
show issu message types	Displays the formats, versions, and size of ISSU messages supported by a particular client.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu entities

To display information about entities within one or more In Service Software Upgrade (ISSU) clients, use the **show issu entities** command in user EXEC or privileged EXEC mode.

show issu entities [*client_id*]

Note An entity is a logical group of sessions that possess some common attributes.

Syntax Description

client_id	(Optional) The identification number of a single ISSU client.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Enter a Client_ID if you are interested in seeing information only about one client's entities. If a Client_ID is not specified, the command will display all ISSU clients' entities known to the device.

If you are not sure of the precise Client_ID number to enter for the client you are interested in, use the **show issu clients** command to display the current list of clients with their names and ID numbers.

Examples

The following example shows detailed information about the entities within the virtual routing and forwarding (VRF) ("Table ID") client:

```
Router# show issu entities 2008

Client_ID = 2008 :
      Entity_ID = 1,  Entity_Name = Tableid Entity :
         MsgType MsgGroup CapType CapEntry CapGroup
          Count    Count   Count   count    Count
            2      2       1       2        2
```

Table 81 show issu entities Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for the specified client.
Entity_ID	The identification number used by ISSU for each entity within this client.
Entity_Name	A character string describing the entity.

Table 81 show issu entities Field Descriptions (continued)

Field	Description
MsgType Count	The number of message types within the identified entity.
MsgGroup Count	The number of message groups within the identified entity. A message group is a list of message types.
CapType Count	The number of capability types within the identified entity.
CapEntry Count	The number of capability entries within the identified entity. A capability entry is a list of all mutually dependent capability types within a particular client session and, optionally, other capability types belonging to that client session.
CapGroup Count	The number of capability groups within the identified entity. A capability group is a list of capability entries given in priority sequence.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications and protocols on this network supported by ISSU.
show issu sessions	Displays detailed information about a particular ISSU client—including whether the client status for the impending software upgrade is COMPATIBLE.

show issu message types

To display formats (“types”), versions, and maximum packet size of the In Service Software Upgrade (ISSU) messages supported by a particular client, use the **show issu message types** command in user EXEC or privileged EXEC mode.

show issu message types *client-id*

Syntax Description

client-id	The identification number used by ISSU for a client application.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If you are not sure of the Client_ID number to enter into this command, use the **show issu clients** command. It displays the current list of clients, along with their names and ID numbers.

Examples

The following example displays the message type, version, and maximum message size supported by the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) client:

```
Router# show issu message types 2009

Client_ID = 2009,  Entity_ID = 1 :
   Message_Type = 1,  Version_Range = 1 ~ 1
         Message_Ver = 1,    Message_Mtu = 32
```

Table 82 describes the significant fields shown in the display.

Table 82 show issu message types Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for this client.
Entity_ID	The identification number used by ISSU for this entity.
Message_Type	An identification number that uniquely identifies the format used in the ISSU messages conveyed between the two endpoints.
Version_Range	The lowest and highest message-version numbers contained in the client application.

Table 82 show issu message types Field Descriptions (continued)

Field	Description
Message_Ver	Message version. Because each client application contains one or more versions of its messages, ISSU needs to discover these versions and negotiate between the new and old system software which version to use in its preparatory communications.
Message_Mtu	Maximum size (in bytes) of the transmitted message. A value of 0 means there is no restriction on size; fragmentation and reassembly are therefore being handled in a manner transparent to the ISSU infrastructure.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications on this network supported by ISSU.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu negotiated

To display details of the session's negotiation about message version or client capabilities, use the **show issu negotiated** command in user EXEC or privileged EXEC mode.

show issu negotiated {**version** | **capability**} *session-id*

Syntax Description

version	Displays results of a negotiation about versions of the messages exchanged during the specified session, between the active and standby endpoints.
capability	Displays results of a negotiation about the client application's capabilities for the specified session.
session-id	The number used by In Service Software Upgrade (ISSU) to identify a particular communication session between the active and the standby devices.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If you are not sure of the session_ID number to enter into this command, enter the **show issu sessions** command. It will display the session_ID.

Examples

The following example displays the results of a negotiation about message versions:

```
router# show issu negotiated version 39

Session_ID = 39 :
    Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 32
```

Table 83 describes the significant fields shown in the display.

Table 83 show issu negotiated version Field Descriptions

Field	Description
Session_ID	The identification number of the session being reported on.
Message_Type	An identification number that uniquely identifies the format that was used by the ISSU messages conveyed between the two endpoints.

Table 83 show issu negotiated version Field Descriptions (continued)

Field	Description
Negotiated_Version	The message version that was decided upon, for use during the software upgrade process.
Message_Mtu	Maximum size (in bytes) of the transmitted message. A value of 0 means there is no restriction on size. In that case, fragmentation and reassembly are handled in a manner transparent to the ISSU infrastructure.

The following example displays the results of a negotiation about the client application's capabilities:

```
router# show issu negotiated capability 39

Session_ID = 39 :
     Negotiated_Cap_Entry = 1
```

Table 84 describes the significant fields shown in the display.

Table 84 show issu negotiated capability Field Descriptions

Field	Description
Session_ID	The identification number of the session being reported on.
Negotiated_Cap_Entry	A numeral that stands for a list of the negotiated capabilities in the specified client session.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications on this network supported by ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status is compatible for the impending software upgrade.

show issu sessions

To display detailed information about a particular In Service Software Upgrade (ISSU) client—including whether the client status for the impending software upgrade is compatible—use the **show issu sessions** command in user EXEC or privileged EXEC mode.

show issu sessions *client-id*

Syntax Description

client-id	The identification number used by ISSU for the client.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If you are not sure of the Client_ID number to enter into this command, use the **show issu clients** command to display the current list of clients with their names and ID numbers.

Examples

The following example shows detailed information about the LDP Client:

```
Router# show issu sessions 2011

 Client_ID = 2011,  Entity_ID = 1 :

 *** Session_ID = 46,  Session_Name = LDP Session :

    Peer    Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
     4       34   PRIMARY   COMPATIBLE    1        1         0
                           (no policy)

    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 46
         Nego_Session_Name = LDP Session
         Transport_Mtu = 3948
```

Table 85 describes the significant fields shown in the display.

Table 85 show issu sessions Field Descriptions

Field	Description
Client_ID	The identification number used by ISSU for that client.
Entity_ID	The identification number used by ISSU for each entity within this client.
Session_ID	The identification number used by ISSU for this session.
Session_Name	A character string describing the session.
Peer UniqueID	An identification number used by ISSU for a particular endpoint, such as a Route Processor or line card (could be a value based on slot number, for example). The peer that has the smaller unique_ID becomes the Primary (initiating) side in the capability and message version negotiations.
Peer Sid	Peer session ID.
Negotiate Role	Negotiation role of the endpoint: either PRIMARY (in which case the device initiates the negotiation) or PASSIVE (in which case the device responds to a negotiation initiated by the other device).
Negotiated Result	The features (“capabilities”) of this client’s new software were found to be either COMPATIBLE or INCOMPATIBLE with the intended upgrade process. (“Policy” means that an override of the negotiation result has been allowed by the software. Likewise, “no policy” means that no such override is present to be invoked).
Cap GroupID	Capability group ID: the identification number used for a list of distinct functionalities that the client application contains.
Msg GroupID	Message group ID: the identification number used for a list of formats employed when conveying information between the active device and the standby device.
Session Signature	Session signature: a unique ID to identify a current session in a shared negotiation scenario.
Nego_Session_ID	Negotiation session ID: the identification number used by ISSU for this negotiation session.
Nego_Session_Name	Negotiation session name: a character string describing this negotiation session.
Transport_Mtu	Maximum packet size (in bytes) of the ISSU messages conveyed between the two endpoints. A value of 0 means there is no restriction on size; in this case, fragmentation and reassembly then are handled in a manner transparent to the ISSU infrastructure.

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients—that is, the applications on this network supported by ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.

show mpls atm-ldp bindings

Note Effective with Cisco IOS Release 12.4(20)T, the **show mpls atm-ldp bindings** command is not available in Cisco IOS software.

To display specified entries from the ATM label binding database, use the **show mpls atm-ldp bindings** command in privileged EXEC mode.

show mpls atm-ldp bindings [*network* {*mask* | *length*}] [**local-label** *vpi vci*] [**remote-label** *vpi vci*] [**neighbor** *interface*]

Syntax Description

network	(Optional) Defines the destination network number.
mask	(Optional) Defines the network mask in the form A.B.C.D (destination prefix).
length	(Optional) Defines the mask length (1 to 32).
local-label *vpi vci*	(Optional) Selects the label values assigned by this router. The virtual path identifier (VPI) range is 0 to 4095. The virtual channel identifier (VCI) range is 0 to 65535.
remote-label *vpi vci*	(Optional) Selects the label values assigned by the other router. VPI range is 0 to 4095. VCI range is 0 to 65535.
neighbor *interface*	(Optional) Selects the label values assigned by the neighbor on a specified interface.

Command Default

The entire ATM label binding database is displayed if no optional arguments or keywords are specified.

Note To display information about entries in the label binding database for interfaces other than ATM interfaces, use the **show mpls ip binding** command.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to use Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	The VPI range of values for this command was extended to 4095.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Release	Modification
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

The ATM label binding database contains entries for label virtual circuits (VCs) on label-controlled (LC)-ATM interfaces. Command output can show a summary of entries from the entire database, or the output can be limited to a subset of entries based on the following:

- Specific prefix
- Specific VC label value
- Specific assigning interface

Note This command displays ATM label bindings learned by the Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP). TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(27)SBC and later 12.2S releases, and 12.3(14)T and later releases.

Note The **show mpls ip binding** command includes the output generated by the **show mpls atm-ldp bindings** command and information about label bindings for packet interfaces.

Examples

The following is sample output from the **show mpls atm-ldp bindings** command:

```
Router# show mpls atm-ldp bindings

 Destination: 10.24.0.0/24
    Tailend Router ATM1/0.1 1/39 Active, VCD=3
 Destination: 10.15.0.15/32
    Tailend Router ATM1/0.1 1/33 Active, VCD=4
 Destination: 10.0.7.7/32
    Headend Router ATM1/0.1 (2 hops) 1/34  Active, VCD=810
```

The following is sample output from the **show mpls atm-ldp bindings** command on an ATM switch:

```
Router# show mpls atm-ldp bindings

Destination: 172.16.0.0/16
    Tailend Switch ATM0/0/3 1/35 Active -> Terminating Active
Destination: 10.4.4.4/32
    Transit ATM0/0/3 1/33 Active -> ATM0/1/1 1/33 Active
```

Table 86 describes the significant fields shown in the displays.

Table 86 show mpls atm-ldp bindings Field Descriptions

Field	Description
Destination	Destination (network/mask).
Headend Router Tailend Router Tailend Switch Transit	Indicates types of VCs. Options are the following: • Tailend—VC that terminates at this platform • Headend—VC that originates at this router • Transit—VC that passes through a switch
ATM1/0.1	ATM interface.
1/35	VPI/VCI.
Active	Indicates VC state. Options include the following: • Active—Set up and working • Bindwait—Waiting for a response • Remote Resource Wait—Waiting for resources (VPI/VCI space) to be available on the downstream device • Parent Wait—Transit VC input side waiting for output side to become active
VCD=3	Virtual circuit descriptor number.

Related Commands

Command	Description
show mpls ip binding	Displays specified information about label bindings learned by the MPLS LDP.

show mpls atm-ldp bindwait

Note Effective with Cisco IOS Release 12.4(20)T, the **show mpls atm-ldp bindwait** command is not available in Cisco IOS software.

To display the number of bindings waiting for label assignments from a remote Multiprotocol Label Switching (MPLS) ATM switch, use the **show mpls atm-ldp bindwait** command in privileged EXEC mode.

show mpls atm-ldp bindwait

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was modified to use MPLS Internet Engineering Task Force (IETF) command syntax and terminology.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(20)T	This command was removed.

Usage Guidelines

Use this command to display information about virtual circuits (VCs) in the bindwait state.

Examples

The following is sample output from the **show mpls atm-ldp bindwait** command:

```
Router# show mpls atm-ldp bindwait

Waiting for bind on ATM1/0.2
  10.3.3.1/32          10.3.3.1/32          10.3.3.2/32
  10.3.3.2/32          10.3.3.3/32          10.3.3.3/32
  10.3.3.4/32          10.3.3.4/32          10.3.3.5/32
  10.3.3.5/32          10.3.3.6/32          10.3.3.6/32
  10.3.3.7/32          10.3.3.7/32          10.3.3.8/32
  10.3.3.8/32          10.3.3.9/32          10.3.3.9/32
.
.
.
```

```
end
```

If there are no bindings waiting for label assignments from the remote MPLS ATM switch, this command does not display any output.

Related Commands

Command	Description
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.

show mpls atm-ldp capability

Note Effective with Cisco IOS Release 12.4(20)T, the **show mpls atm-ldp capability** command is not available in Cisco IOS software.

To display the Multiprotocol Label Switching (MPLS) ATM capabilities negotiated with Label Distribution Protocol (LDP) neighbors for label-controlled (LC)-ATM interfaces, use the **show mpls atm-ldp capability** command in privileged EXEC mode.

show mpls atm-ldp capability

Syntax Description

This command has no arguments or keywords.

Command Default

This command always displays all the MPLS ATM capabilities negotiated with all the LDP neighbors.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to use MPLS Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.4(20)T	This command was removed.

Usage Guidelines

When two label switch routers (LSRs) establish an LDP session, they negotiate parameters for the session, such as the range of virtual path identifiers (VPIs) and virtual channel identifiers (VCIs) that will be used as labels.

This command displays the MPLS ATM capabilities negotiated by LDP or the Tag Distribution Protocol (TDP).

Note TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(27)SBC and later 12.2S releases, and 12.3(14)T and later releases.

Examples

The following is sample output from the **show mpls atm-ldp capability** command:

```
Router# show mpls atm-ldp capability

               VPI           VCI           Alloc   Odd/Even  VC Merge
ATM0/1/0       Range         Range         Scheme  Scheme    IN   OUT
  Negotiated   [100 - 101]   [33 - 1023]   UNIDIR            -    -
  Local        [100 - 101]   [33 - 16383]  UNIDIR            EN   EN
  Peer         [100 - 101]   [33 - 1023]   UNIDIR            -    -

               VPI           VCI           Alloc   Odd/Even  VC Merge
ATM0/1/1       Range         Range         Scheme  Scheme    IN   OUT
  Negotiated   [201 - 202]   [33 - 1023]   BIDIR             -    -
  Local        [201 - 202]   [33 - 16383]  UNIDIR  ODD       NO   NO
  Peer         [201 - 202]   [33 - 1023]   BIDIR   EVEN      -    -
```

Table 87 describes the significant fields shown in the display.

Table 87 show mpls atm-ldp capability Field Descriptions

Field	Description
VPI Range	Minimum and maximum numbers of VPIs supported on this interface.
VCI Range	Minimum and maximum numbers of VCIs supported on this interface.
Alloc Scheme	Indicates the applicable allocation scheme, as follows: • UNIDIR—Unidirectional capability indicates that the peer can, within a single VPI, support binding of the same VCI to different prefixes on different directions of the link. • BIDIR—Bidirectional capability indicates that within a single VPI, a single VCI can appear in one binding only. In this case, one peer allocates bindings in the even VCI space, and the other in the odd VCI space. The system with the lower LDP identifier assigns even-numbered VCIs. The negotiated allocation scheme is UNIDIR, only if both peers have UNIDIR capability. Otherwise, the allocation scheme is BIDIR. **Note** These definitions for *unidirectional* and *bidirectional* are consistent with normal ATM usage of the terms; however, they are exactly opposite from the definitions for them in the IETF LDP specification.
Odd/Even Scheme	Indicates whether the local device or the peer is assigning an odd- or even-numbered VCI when the negotiated scheme is BIDIR. It does not display any information when the negotiated scheme is UNIDIR.

Table 87 show mpls atm-ldp capability Field Descriptions (continued)

Field	Description
VC Merge	Indicates the type of virtual circuit (VC) merge support available on this interface. There are two possibilities, as follows: • IN—Indicates the input interface merge capability. IN accepts the following values: – EN—The hardware interface supports VC merge, and VC merge is enabled on the device. – DIS—The hardware interface supports VC merge and VC merge is disabled on the device. – NO—The hardware interface does not support VC merge. • OUT—Indicates the output interface merge capability. OUT accepts the same values as the input merge side. The VC merge capability is meaningful only on ATM switches. This capability is not negotiated.
Negotiated	Indicates the set of options that both LDP peers have agreed to share on this interface. For example, the VPI or VCI allocation on either peer remains within the negotiated range.
Local	Indicates the options supported locally on this interface.
Peer	Indicates the options supported by the remote LDP peer on this interface.

Related Commands

Command	Description
mpls ldp atm vc-merge	Controls whether the vc-merge (multipoint-to-point) is supported for unicast label VCs.

sshow mpls atm-ldp summary

Note Effective with Cisco IOS Release 12.4(20)T, the **show mpls atm-ldp summary** command is not available in Cisco IOS software.

To display summary information about all the entries in the ATM label binding database, use the **show mpls atm-ldp summary** command in privileged EXEC mode.

show mpls atm-ldp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to use Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(20)T	This command was removed.

Usage Guidelines

Use this command to display dynamic ATM accounting information.

Examples

The following is sample output from the **show mpls atm-ldp summary** command:

```
Router# show mpls atm-ldp summary

Total number of destinations: 406

ATM label bindings summary
interface      total   active  local   remote  Bwait   Rwait   IFwait
```

```
ATM0/0/0        406     406     404     2       0       0       0
ATM0/0/1        406     406     3       403     0       0       0
```

Table 88 describes the significant fields shown in the display.

Table 88 show mpls atm-ldp summary Field Descriptions

Field	Description
Total number of destinations:	Number of known destination address prefixes.
interface	Name of an interface with associated ATM label bindings.
total	Total number of ATM labels on this interface.
active	Number of ATM labels in an “active” state that are ready to use for data transfer.
local	Number of ATM labels assigned by this label switch router (LSR) on this interface.
remote	Number of ATM labels assigned by the neighbor LSR on this interface.
Bwait	Number of bindings that are waiting for a label assignment from the neighbor LSR.
Rwait	Number of bindings that are waiting for resources (virtual path identifier [VPI] /virtual channel identifier [VCI] space) to be available on the downstream device.
IFwait	Number of bindings that are waiting for learned labels to be installed for switching use.

Related Commands

Command	Description
show isis database verbose	Displays the requested entries from the ATM LDP label binding database.

show mpls cos-map

Note Effective with Cisco IOS Release 12.4(20)T, the **show mpls cos-map** command is not available in Cisco IOS software.

To display the quality of service (QoS) map used to assign a quantity of label virtual circuits and the associated class of service (CoS) for those virtual circuits, use the **show mpls cos-map** command in privileged EXEC mode.

show mpls cos-map [*cos-map*]

Syntax Description

cos-map	(Optional) Number specifying the QoS map to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to match Multiprotocol Label Switching (MPLS) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	The heading in the output was changed from tag-vc to label-vc.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(20)T	This command was removed.

Usage Guidelines

Not entering a specific QoS number causes all QoS maps to be displayed.

Note Cisco 10000 series routers do not use the **show mpls cos-map** command.

Examples

The following is sample output from the **show mpls cos-map** command:

```
Router# show mpls cos-map 2

cos-map 2    class  Label-VC
             3      control
             2      control
             1      available
             0      available
```

Table 89 describes the significant fields shown in the display.

Table 89 show mpls cos-map Field Descriptions

Field	Description
cos-map	Configures a class map, which specifies how classes map to MPLS virtual circuits when they are combined with a prefix map.
class	The IP precedence.
Label-VC	An ATM virtual circuit that is set up through ATM label switch router (LSR) label distribution procedures.

Related Commands

Command	Description
mpls cos-map	Creates a class map specifying how classes map to label virtual circuits when they are combined with a prefix map.

show mpls flow mappings

To display all entries in the Multiprotocol Label Switching (MPLS) Prefix/Application/Label (PAL) table, use the **show mpls flow mappings** command in user EXEC mode or privileged EXEC mode.

show mpls flow mappings

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you are interested in only a certain type of MPLS label and do not want to display the entire MPLS PAL table, you can use the **show mpls flow mappings** | **include** *label-type* command.

Examples

The following sample output from the **show mpls flow mappings** command displays all entries in the MPLS PAL table:

```
Router# show mpls flow mappings

Label    Owner    Route-Distinguisher Prefix          Allocated
18       LDP                          10.0.0.5        00:52:10
21       BGP                          0.0.0.0         00:52:18
22       BGP                          0.0.0.0         00:52:18
25       BGP                          0.0.0.0         00:51:44
26       LDP                          10.32.0.0       00:52:10
27       TE-MIDPT                     10.30.0.2       00:52:06
28       LDP                          10.33.0.0       00:52:10
29       LDP                          10.0.0.1        00:52:10
30       LDP                          10.0.0.3        00:52:10
```

In this example, the **mpls export vpnv4 prefixes** command was not configured. Therefore, the MPLS PAL table did not export a route distinguisher for the Border Gateway Protocol (BGP) application, and the associated prefix is exported as 0.0.0.0.

Table 90 describes the significant fields shown in the display.

Table 90 show mpls flow mappings Field Descriptions

Field	Description
Label	Value given to the MPLS label by the router.
Owner	MPLS application that allocated the label. • LDP = Label Distribution Protocol • BGP = Border Gateway Protocol • TE-MIDT = Traffic engineering tunnel midpoint
Route-Distinguisher	Value (8-byte) that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix.
Prefix	Prefix used by the router to route data to the destination address.
Allocated	System uptime at which the MPLS PAL mapping record was created.

The following is sample output from the **show mpls flow mappings** command if you previously entered the **mpls export vpnv4 prefixes** command:

```
# show mpls flow mappings

Label    Owner    Route-Distinguisher Prefix          Allocated
16       LDP                          10.0.0.3        00:58:03
17       LDP                          10.33.0.0       00:58:03
19       TE-MIDPT                     10.30.0.2       00:58:06
20       LDP                          10.0.0.5        00:58:03
23       LDP                          10.0.0.1        00:58:03
24       LDP                          10.32.0.0       00:58:03
27       BGP      100:1               10.34.0.0       00:57:48
31       BGP      100:1               10.0.0.9        00:58:21
32       BGP      100:1               10.3.3.0        00:58:21
```

The following sample output from the **show mpls flow mappings** | **include LDP** command displays only MPLS PAL entries that were allocated by LDP:

```
Router# show mpls flow mappings | include LDP

Label    Owner    Route-Distinguisher Prefix          Allocated
16       LDP                          10.0.0.3        00:58:03
17       LDP                          10.33.0.0       00:58:03
20       LDP                          10.0.0.5        00:58:03
23       LDP                          10.0.0.1        00:58:03
24       LDP                          10.32.0.0       00:58:03
```

Related Commands

Command	Description
show ip cache verbose flow	Displays a detailed summary of NetFlow statistics.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

show mpls forwarding vrf

To display label forwarding information for advertised Virtual Private Network (VPN) routing and forwarding (VRF) instance routes, use the **show mpls forwarding vrf** command in privileged EXEC mode. To disable the display of label forwarding information, use the **no** form of this command.

show mpls forwarding vrf *vrf-name* [*ip-prefix/length* [*mask*]] [**detail**] [*output-modifiers*]

no show mpls forwarding vrf *vrf-name* [*ip-prefix/length* [*mask*]] [**detail**] [*output-modifiers*]

Syntax Description

vrf-name	Displays network layer reachability information (NLRI) associated with the named VRF.
ip-prefix/length	(Optional) IP prefix address (in dotted decimal format) and length of mask (0 to 32).
mask	(Optional) Destination network mask, in dotted decimal format.
detail	(Optional) Displays detailed information on the VRF routes.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was modified to reflect new Multiprotocol Label Switching (MPLS) Internet Engineering Taskforce (IETF) terminology and CLI command syntax and was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(22)S	The command output was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display label forwarding entries associated with a particular VRF or IP prefix.

Examples

The following example shows label forwarding entries that correspond to the VRF called vpn1:

```
Router# show mpls forwarding vrf vpn1 detail

Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
35     24 10.0.0.0/8[V]     0          Et0/0/4 10.0.0.1
        MAC/Encaps=14/22, MRU=1496, Tag Stack{24 19}
        00D006FEDBE100D0974988048847 0001800000013000
        VPN route: vpn1
        No output feature configured
    Per-packet load-sharing
```

Related Commands

Command	Description
show ip cef vrf	Displays VRFs and associated interfaces.
show mpls forwarding-table	Displays the contents of the LFIB.

show mpls forwarding-table

To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB), use the **show mpls forwarding-table** command in privileged EXEC mode.

show mpls forwarding-table [*network* {*mask* | *length*} | **labels** *label* [**-** *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]

Syntax Description

network	(Optional) Destination network number.
mask	IP address of the destination mask whose entry is to be shown.
length	Number of bits in the mask of the destination.
labels *label* **-** *label*	(Optional) Displays only entries with the specified local labels.
interface *interface*	(Optional) Displays only entries with the specified outgoing interface.
next-hop *address*	(Optional) Displays only entries with the specified neighbor as the next hop.
lsp-tunnel	(Optional) Displays only entries with the specified Label Switched Path (LSP) tunnel, or with all LSP tunnel entries.
tunnel-id	(Optional) Specifies the LSP tunnel for which to display entries.
vrf *vrf-name*	(Optional) Displays only entries with the specified VPN routing and forwarding (VRF) instance.
detail	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit (MTU), and all labels).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was updated with MPLS terminology and command syntax.
12.2(8)T	The command was modified to accommodate use of the MPLS experimental (EXP) level as a selection criterion for packet forwarding. The output display was modified to include a bundle adjacency field and exp (VCD) values when the optional **detail** keyword is specified.
12.0(22)S	IPv6 MPLS aggregate label and prefix information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(27)S	The command output was modified to include explicit-null label information.
12.2(25)S	The output was changed in the following ways: • The term “tag” was replaced with the term “label.” • The term “untagged” was replaced with the term “no label.”
12.0(29)S	This command was integrated into Cisco IOS Release 12.0(29)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The command output was modified for the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature to show the status of local labels in holdown. The status indicator showing that traffic is forwarded through an LSP tunnel is moved to the local label.

Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
26    No Label      10.253.0.0/16     0         Et4/0/0       10.27.32.4
28    1/33          10.15.0.0/16      0         AT0/0.1       point2point
29    Pop Label     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    No Label[T]   10.100.100.101/32 0         Tu301         point2point
36    Pop Label     10.1.0.0/16      0         Hs5/0         point2point
      1/37          10.1.0.0/16      0         AT0/0.1       point2point

[T]     Forwarding through a TSP tunnel.
        View additional labeling info with the 'detail' option
```

The following is sample output from the **show mpls forwarding-table** command when the IPv6 Provider Edge Router over MPLS feature is configured to allow IPv6 traffic to be transported across an IPv4 MPLS backbone. The labels are aggregated because there are several prefixes for one local label, and the prefix column contains “IPv6” instead of a target prefix.

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
16    Aggregate     IPv6              0
17    Aggregate     IPv6              0
18    Aggregate     IPv6              0
19    Pop Label     192.168.99.64/30  0         Se0/0         point2point
20    Pop Label     192.168.99.70/32  0         Se0/0         point2point
21    Pop Label     192.168.99.200/32 0         Se0/0         point2point
22    Aggregate     IPv6              5424
23    Aggregate     IPv6              3576
24    Aggregate     IPv6              2600
```

The following is sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword. If the MPLS EXP level is used as a selection criterion for packet forwarding, a bundle adjacency exp (vcd) field is included in the display. This field includes the EXP value and the corresponding Virtual Circuit Descriptor (VCD) in parentheses. The line in the output that reads “No output feature configured” indicates that the MPLS egress NetFlow accounting feature is not enabled on the outgoing interface for this prefix.

```
Router# show mpls forwarding-table detail

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
label   label or VC     or Tunnel Id      switched  interface
16    Pop label       10.0.0.6/32        0         AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
17    18            10.0.0.9/32        0         AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{18}
      00010000AAAA030000008847 00012000
      No output feature configured
18    19            10.0.0.10/32        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{19}
      00010000AAAA030000008847 00013000
      No output feature configured
19    17            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{17}
      00010000AAAA030000008847 00011000
      No output feature configured
20    20            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{20}
      00010000AAAA030000008847 00014000
      No output feature configured
21    Pop label       10.0.0.0/24        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
22    Pop label       10.0.0.4/32         0        Et2/3         10.0.0.4
      MAC/Encaps=14/14, MTU=1504, label Stack{}
      000427AD10430005DDFE043B8847
      No output feature configured
```

The following is sample output from the **show mpls forwarding-table** command when you use the **detail** keyword. In this example, the MPLS egress NetFlow accounting feature is enabled on the first three prefixes, as indicated by the line in the output that reads “Feature Quick flag set.”

```
Router# show mpls forwarding-table detail

Local  Outgoing    Prefix            Bytes label  Outgoing   Next Hop
label    label or VC   or Tunnel Id      switched   interface
16     Aggregate   10.0.0.0/8[V]     0
        MAC/Encaps=0/0, MTU=0, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
17     No label    10.0.0.0/8[V]      0          Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
```

```
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
18     No label    10.42.42.42/32[V] 4185       Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
19     2/33        10.41.41.41/32    0          AT1/0/0.1  point2point
        MAC/Encaps=4/8, MTU=4470, label Stack{2/33(vcd=2)}
        00028847 00002000
        No output feature configured
```

Cisco 10000 Series Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        Pop Label     10.0.0.0/8        0             Fa1/1/0    10.0.0.2
17      Aggregate     10.0.0.0/8[V]     570           vpn2
21      Pop Label     10.11.11.11/32    0             Fa1/0/0    10.0.0.2
22      Pop Label     10.12.12.12/32    0             Fa1/1/0    10.0.0.2
23      No Label      10.3.0.0/16[V]     0             Fa4/1/0   10.0.0.2
```

The following is Cisco 10000 series sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword:

```
Router# show mpls forwarding-table detail

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C93889000B45C930218847
        No output feature configured
        Pop Label     10.0.0.0/8        0             Fa1/1/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C92881000B45C930288847
        No output feature configured
17      Aggregate    10.0.0.0/8[V]      570           vpn2
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        VPN route: vpn2
        No output feature configured
21      Pop Label     10.11.11.11/32     0            Fa1/0/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
       000B45C93889000B45C930218847
       No output feature configured
```

Table 91 describes the significant fields in the sample output.

Table 91 show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing Label or VC **Note** This field is not supported on the Cisco 10000 series routers.	Label assigned by the next hop or Virtual Path Identifier (VPI)/ Virtual Channel Identifier (VCI) used to get to next hop. The entries in this column are the following: • [T]—Means forwarding through an LSP tunnel. • No Label—Means that there is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface. • Pop Label—Means that the next hop advertised an implicit NULL label for the destination and that the router removed the top label. • Aggregate—Means there are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, “IPv6” is displayed here. [V]—means that the corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.
Bundle adjacency exp(vcd)	Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD.
MAC/Encaps	Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header.
MTU	MTU of the labeled packet.
label Stack	All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown. **Note** TC-ATM is not supported on Cisco 10000 series routers.
00010000AAAA030000008847 00013000	The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header.

Explicit-Null Label Example

The following example shows output, including the explicit-null label = 0 (commented in bold), from the **show mpls forwarding-table** command on a CSC-PE router:

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix            Bytes label  Outgoing   Next Hop
label  label or VC   or Tunnel Id      switched     interface
17     Pop label     10.10.0.0/32      0            Et2/0      10.10.0.1
18     Pop label     10.10.10.0/24     0            Et2/0      10.10.0.1
19     Aggregate     10.10.20.0/24[V]  0
20     Pop label     10.10.200.1/32[V] 0            Et2/1      10.10.10.1
21     Aggregate     10.10.1.1/32[V]   0
22     0             192.168.101.101/32[V]   \
                                       0            Et2/1      192.168.101.101
23     0             192.168.101.100/32[V]   \
                                       0            Et2/1      192.168.101.100
25     0             192.168.102.125/32[V] 0        Et2/1      192.168.102.125 !outlabel
value 0
```

Table 92 describes the significant fields in the sample output.

Table 92 show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing label or VC	Label assigned by the next hop or VPI/VCI used to get to next hop. The entries this column are the following: • [T]—Means forwarding through an LSP tunnel. • No label—Means that there is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface. • Pop label—Means that the next hop advertised an implicit NULL label for the destination and that this router popped the top label. • Aggregate—Means there are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network. • 0—Means the explicit null label value = 0.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are going. **Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, IPv6 is displayed here. [V]—means that the corresponding prefix is in a VRF.
Bytes label switched	Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.

Cisco IOS Software Modularity: MPLS Layer 3 VPNs Example

The following is sample output from the **show mpls forwarding-table** command.

```
Router# show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  IPv4 VRF[V]      62951000      aggregate/v1
17    [H]  No Label   10.1.1.0/24      0             AT1/0/0.1 point2point
           No Label   10.1.1.0/24      0             PO3/1/0 point2point
      [T]  No Label   10.1.1.0/24      0             Tu1 point2point
18    [HT] Pop Label  10.0.0.3/32      0             Tu1 point2point
19    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
20    [H]  No Label   10.0.0.0/8       0             AT1/0/0.1 point2point
           No Label   10.0.0.0/8       0             PO3/1/0 point2point
21    [H]  No Label   10.0.0.1/32      812           AT1/0/0.1 point2point
           No Label   10.0.0.1/32      0             PO3/1/0 point2point
22    [H]  No Label   10.1.14.0/24     0             AT1/0/0.1 point2point
           No Label   10.1.14.0/24     0             PO3/1/0 point2point
23    [HT] 16         172.1.1.0/24[V]  0             Tu1 point2point
24    [HT] 24         10.0.0.1/32[V]   0             Tu1 point2point
25    [H]  No Label   10.0.0.0/8[V]    0             AT1/1/0.1 point2point
26    [HT] 16         10.0.0.3/32[V]   0             Tu1 point2point
27         No Label   10.0.0.1/32[V]   0             AT1/1/0.1 point2point

[T]     Forwarding through a TSP tunnel.
        View additional labelling info with the 'detail' option
[H]     Local label is being held down temporarily.
```

Table 93 describes the field relating to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature as shown in the sample output.

Table 93 show mpls forwarding-table Field Descriptions

Field	Description
Local label	Label assigned by this router. • [H]—Local labels are in holddown, which means that the application that requested the labels no longer needs them and stops advertising them to its labeling peers. The label's forwarding-table entry is deleted after a short, application-specific time. If any application starts advertising a held-down label to its labeling peers, the label could come out of holddown. **Note** [H] is not shown if labels are held down globally. A label enters global holddown after a stateful switchover or a restart of certain processes in a Cisco IOS modularity environment. • [T]—The label is forwarded through an LSP tunnel. **Note** Although [T] is still a property of the outgoing interface, it is shown in the Local label column. • [HT]—Both conditions apply.

Related Commands

Command	Description
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.

show mpls interfaces

To display information about one or more or all interfaces that are configured for label switching, use the **show mpls interfaces** command in user EXEC or privileged EXEC mode.

show mpls interfaces [*interface* | **vrf** *vpn-name*] [**all**] [**detail**] [**internal**]

Syntax Description

interface	(Optional) Defines the interface about which to display label switching information.
vrf *vpn-name*	(Optional) Displays information about the interfaces that have been configured for label switching for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vpn-name)*.
all	(Optional) When the **all** keyword is specified alone in this command, information about the interfaces configured for label switching is displayed for all VPNs, including the VPNs in the default routing domain.
detail	(Optional) Displays detailed label switching information.
internal	(Optional) Indicates whether Multiprotocol Label Switching (MPLS) egress NetFlow accounting is enabled.

Defaults

If no optional keyword or argument is specified in this command, summary information is displayed for each interface that has been configured for label switching in the default routing domain.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.1(3)T	This command was updated with MPLS command syntax and terminology.
12.0(10)ST	The **internal** keyword was added.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	This command was modified to show Border Gateway Protocol (BGP) and static routing information.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command shows MPLS information about the specified interface, or about all the interfaces for which MPLS has been configured.

If no optional keyword or argument is specified in this command, summary information is displayed for each interface configured for label switching.

Examples

The following is sample output from the **show mpls interfaces** command:

```
Router# show mpls interfaces

Interface              IP         Tunnel   Operational
Ethernet1/1/1          Yes (tdp)  No       No
Ethernet1/1/2          Yes (tdp)  Yes      No
Ethernet1/1/3          Yes (tdp)  Yes      Yes
POS2/0/0               Yes (tdp)  No       No
ATM0/0.1               Yes (tdp)  No       No          (ATM labels)
ATM3/0.1               Yes (ldp)  No       Yes         (ATM labels)
ATM0/0.2               Yes (tdp)  No       Yes
```

Cisco 10000 Series Example

The following is sample output from the **show mpls interfaces** command:

```
Router# show mpls interfaces

Interface                   IP           Tunnel   BGP Static Operational
GigabitEthernet1/0/0        Yes          No       No  No     No
GigabitEthernet2/0/0        No           No       No  Yes    No
GigabitEthernet3/0/0        No           Yes      No  No     No
```

Note If an interface uses LC-ATM procedures, the associated line in the display is flagged with the notation (ATM labels).

Table 94 describes the significant fields shown in the display.

Table 94 show mpls interfaces Field Descriptions

Field	Description
Interface	Interface name.
IP	If IP label switching (sometimes called hop-by-hop label switching) is enabled on this interface, the column entry is “Yes.” Otherwise, the entry is “No.”
Tunnel	If label switched path (LSP) tunnel labeling is on this interface, the column entry is “Yes.” Otherwise, the entry is “No.”
BGP	If BGP has been enabled, the column entry is “Yes.” Otherwise, the entry is “No.”
Static	If static routes have been enabled, the column entry is “Yes.” Otherwise, the entry is “No.”
Operational	If packets are being labeled, the column entry is “Yes.” Otherwise, the entry is “No.”

The following is sample output from the **show mpls interfaces** command with the **detail** keyword:

```
Router# show mpls interfaces detail

Interface Ethernet1/1/1:
        IP labeling enabled (tdp)
        LSP Tunnel labeling not enabled
        MPLS operational
        MPLS turbo vector
        MTU = 1500
Interface POS2/0/0:
        IP labeling enabled (ldp)
        LSP Tunnel labeling not enabled
        MPLS not operational
        MPLS turbo vector
        MTU = 4470
Interface ATM3/0.1:
        IP labeling enabled (ldp)
        LSP Tunnel labeling not enabled
        MPLS operational
        MPLS turbo vector
        MTU = 4470
        ATM labels: Label VPI = 1
                Label VCI range = 33 - 65535
                Control VC = 0/32
```

Cisco 10000 Series Example

The following example is sample output of the **show mpls interfaces** command with the **detail** keyword:

```
Router# show mpls interfaces detail

Interface GigabitEthernet1/0/0:
         IP labeling enabled (ldp)
         LSP Tunnel labeling not enabled
         MPLS operational
         MTU = 1500
Interface POS2/0/0:
         IP labeling enabled (ldp)
         LSP Tunnel labeling not enabled
         MPLS not operational
         MTU = 4470
```

Table 95 describes the significant fields shown in the display.

Table 95 show mpls interfaces detail Field Descriptions

Field	Description
Interface	Interface name.
IP labeling	If IP label switching is enabled on this interface, the entry is “enabled.” Otherwise, the entry is “not enabled.” The output also shows whether LDP or TDP is being used.
LSP Tunnel labeling	If the LSP tunnel labeling is enabled on this interface, the entry is “enabled.” Otherwise, the entry is “not enabled.”
MPLS	If packets are labeled, the entry is “operational.” Otherwise, the entry is “not operational.”
BGP	If BGP has been enabled, the entry is “enabled.” Otherwise, the entry is “not enabled.”

Table 95 show mpls interfaces detail Field Descriptions (continued)

Field	Description
MTU	The setting of the maximum transmission unit, in bytes.
ATM labels: Label VPI	The virtual path identifier (VPI). **Note** This field does not apply to the Cisco 10000 series routers.
Label VCI range	The range of values used in the VPI field for label VCs. **Note** This field does not apply to the Cisco 10000 series routers.
Control VC	The values assigned to the control VC. **Note** This field does not apply to the 10000 series routers.

The following is sample output from the **show mpls interfaces** command with the **all** keyword:

```
Router# show mpls interfaces all

Interface              IP           Tunnel   Operational
ATM1/1/0.1             Yes (tdp)    No       Yes

VRF vpn1:
ATM3/0/0.1             Yes (ldp)    No       Yes

VRF vpn2:
ATM3/0/0.2             Yes (ldp)    No       Yes

VRF vpn3:
ATM3/0/0.3             Yes (ldp)    No       Yes

VRF vpn4:
ATM3/0/0.4             Yes (ldp)    No       Yes

VRF vpn5:
ATM3/0/0.5             Yes (ldp)    No       Yes

VRF vpn6:
Interface              IP           Tunnel   Operational
ATM3/0/0.6             Yes (ldp)    No       Yes

VRF vpn7:
ATM3/0/0.7             Yes (ldp)    No       Yes

VRF vpn8:
ATM3/0/0.8             Yes (ldp)    No       Yes

VRF vpn9:
ATM3/0/0.9             Yes (ldp)    No       Yes

VRF vpn10:
ATM3/0/0.10            Yes (ldp)    No       Yes

VRF vpn11:
ATM3/0/0.11            Yes (ldp)    No       Yes

VRF vpn12:
ATM3/0/0.12            Yes (ldp)    No       Yes
.
.
.
```

The following is sample output from the **show mpls interfaces** command with the **internal** keyword. The output shows whether MPLS egress NetFlow accounting is enabled on the interface. If MPLS egress NetFlow accounting is disabled, the Output_feature_state field displays 0x0. If MPLS egress Netflow accounting is enabled, the Output_feature_state field is any number, except 0x0.

```
Router# show mpls interfaces internal

Interface Ethernet0/0/1:
        IP labeling enabled (tdp)
        LSP Tunnel labeling not enabled
        MPLS operational
        IP to Tag Fast Feature Switching Vector
        MPLS turbo vector
        MTU = 1500, status=0x100043, appcount=1
        Output_feature_state=0x0
Interface Ethernet0/0/2:
        IP labeling enabled (tdp)
        LSP Tunnel labeling not enabled
        MPLS operational
        IP to Tag Fast Feature Switching Vector
        MPLS turbo vector
        MTU = 1500, status=0x100043, appcount=1
        Output_feature_state=0x1
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.
mpls label protocol (global configuration)	Specifies the default label distribution protocol for a platform.
mpls label protocol (interface configuration)	Specifies the label distribution protocol to be used on a given interface.
mpls traffic-eng tunnels (global configuration)	Enables MPLS traffic engineering tunnel signaling on a device.
mpls traffic-eng tunnels (interface configuration)	Enables MPLS traffic engineering tunnel signaling on an interface.

show mpls ip binding

To display specified information about label bindings learned by the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), use the **show mpls ip binding** command in user EXEC or privileged EXEC mode.

show mpls ip binding [**vrf** *vrf-name* | **all**] [*network* {*mask* | *length*} [**longer-prefixes**]] [**neighbor** *address* | **local**] [**local-label** {**atm** *vpi vci* | *label* [**-** *label*]}] [**remote-label** {**atm** *vpi vci* | *label* [**-** *label*]}] [**interfac***e interface*] [**generic** | **atm**]

show mpls ip binding [**vrf** *vrf-name* | **all**] [**detai**l | **summary**]

Cisco 10000 Series Routers

show mpls ip binding [*network* {*mask* | *length*} [**longer-prefixes**]] [**neighbor** *address* | **local**] [**local-label** *label* [**-** *label*]] [**remote-label** *label* [**-** *label*]] [**generic**]

show mpls ip binding [**detail** | **summary**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*). **Note** This keyword and argument pair does not apply to the Cisco 10000 series routers.
all	(Optional) Displays binding information for all VRFs. **Note** This keyword does not apply to the Cisco 10000 series routers.
network	(Optional) Defines the destination network number.
mask	Defines the network mask, written as A.B.C.D.
length	Defines the mask length (1 to 32 characters).
longer-prefixes	(Optional) Selects any prefix that matches the *mask* with a *length* from 1 to 32 characters.
neighbor *address*	(Optional) Displays label bindings assigned by the selected neighbor.
local	(Optional) Displays the local label bindings.
local-label atm *vpi vci*	(Optional) Displays the entry with the locally assigned ATM label that matches the specified ATM label value. The virtual path identifier (VPI) range is 0 to 4095. The virtual channel identifier (VCI) range is 0 to 65535. **Note** These keywords and arguments do not apply to the Cisco 10000 series routers.
local-label *label - label*	(Optional) Displays entries with locally assigned labels that match the specified label values. Use the *label - label* arguments and keyword to indicate the label range. The hyphen (-) keyword is required for a label range.
remote-label atm *vpi vci*	(Optional) Displays entries with remotely assigned ATM label values learned from neighbor routers that match the specified ATM label value. The VPI range is 0 to 4095. The VCI range is 0 to 65535. **Note** These keywords and arguments do not apply to the Cisco 10000 series routers.

remote-label *label - label*	(Optional) Displays entries with remotely assigned labels learned from neighbor routers that match the specified label values. Use the *label - label* arguments and keyword to indicate the label range. The hyphen (-) keyword is required for a label range.
interface *interface*	(Optional) Displays label bindings associated with the specified interface (for label-controlled (LC)-ATM only). **Note** This keyword and argument pair does not apply to the Cisco 10000 series routers.
generic	(Optional) Displays only generic (non-LC-ATM) label bindings.
atm	(Optional) Displays only LC-ATM label bindings. **Note** This keyword does not apply to the Cisco 10000 series routers.
detail	(Optional) Displays detailed information about label bindings learned by LDP.
summary	(Optional) Displays summary information about label bindings learned by LDP.

Defaults

All label bindings are displayed when no optional arguments or keywords are specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	The VPI range of values was extended to 4095.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **detail** keyword was added to display checkpoint status for local label bindings.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show mpls ip binding** command displays label bindings learned by LDP or the Tag Distribution Protocol (TDP).

Note TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(27)SBC and later 12.2S releases, and 12.3(14)T and later releases.

To summarize information about label bindings learned by LDP, use the **show mpls ip binding summary** command in user EXEC or privileged EXEC mode.

A request can specify that the entire database be displayed, that a summary of entries from the database be displayed, or that the display be limited to a subset of entries. The subset can be limited according to any of the following:

- Prefix
- Input or output label values or ranges
- Neighbor advertising the label
- Interface for label bindings of interest (LC-ATM only)

  Note LC-ATM label binding interface does not apply to the Cisco 10000 series routers.

- Generic (non-LC-ATM) label bindings
- LC-ATM label bindings

  Note LC-ATM label binding interface does not apply to the Cisco 10000 series routers.

Examples

The following is sample output from the **show mpls ip binding** command. The output shows all the label bindings in the database.

```
Router# show mpls ip binding

  10.0.0.0/8
        in label:     20
        out label:    26        lsr: 10.0.0.55:0
        out vc label: 1/80      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    ingress 3 hops (vcd 49)
  172.16.0.0/8
        in label:     25
        in vc label:  1/36      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    egress (vcd 55)
        out label:    imp-null  lsr: 10.0.0.55:0     inuse
```

```
  192.168.0.66/32
        in label:     26
        in vc label:  1/39      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    egress (vcd 58)
        out label:    16        lsr: 10.0.0.55:0     inuse
        .
        .
        .
```

In the following example, a request is made for the display of the label binding information for prefix 192.168.44.0/24:

```
Router# show mpls ip binding 192.168.44.0 24

  192.168.44.0/24
        in label:     24
        in vc label:  1/37      lsr: 10.0.7.7:2      ATM1/0.8
                      Active    egress (vcd 56)
        out label:    imp-null  lsr: 10.0.0.55:0     inuse
```

In the following example, the **local-label** keyword is used to request that label binding information be displayed for the prefix with local label 58:

```
Router# show mpls ip binding local-label 58

  192.168.0.0/16
        in label:     58
        out label:    imp-null  lsr: 10.0.0.55:0     inuse
```

The following sample output shows the label bindings for the VPN routing and forwarding instance named vpn1:

```
Router# show mpls ip binding vrf vpn1

  10.3.0.0/16
        in label:    117
        out label:   imp-null  lsr:10.14.14.14:0
  10.13.13.13/32
        in label:    1372
        out label:   268       lsr:10.14.14.14:0
  10.14.14.14/32
        in label:    118
        out label:   imp-null  lsr:10.14.14.14:0
  10.15.15.15/32
        in label:    1370
        out label:   266       lsr:10.14.14.14:0
  10.16.16.16/32
        in label:    8370
        out label:   319       lsr:10.14.14.14:0
  10.18.18.18/32
        in label:    21817
        out label:   571       lsr:10.14.14.14:0
  30.2.0.0/16
        in label:    6943
        out label:   267       lsr:10.14.14.14:0
  10.30.3.0/16
        in label:    2383
        out label:   imp-null  lsr:10.14.14.14:0
  10.30.4.0/16
        in label:    77
        out label:   imp-null  lsr:10.14.14.14:0
  10.30.5.0/16
        in label:    20715
        out label:   504       lsr:10.14.14.14:0
```

```
  10.30.7.0/16
        in label:    17
        out label:   imp-null  lsr:10.14.14.14:0
  10.30.10.0/16
        in label:    5016
        out label:   269       lsr:10.14.14.14:0
  10.30.13.0/16
        in label:    76
        out label:   imp-null  lsr:10.14.14.14:0
```

The following sample output shows label binding information for all VRFs:

```
Router# show mpls ip binding all

  10.0.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.131.0.1:0
  10.11.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.131.0.1:0
  10.101.0.1/32
        out label:    imp-null  lsr: 10.131.0.1:0
  10.131.0.1/32
        in label:     20
        out label:    imp-null  lsr: 10.131.0.1:0      inuse
  10.134.0.1/32
        in label:     imp-null
        out label:    16        lsr: 10.131.0.1:0
VRF vrf1:
  10.0.0.0/24
        out label:    imp-null  lsr: 10.132.0.1:0
  10.11.0.0/24
        out label:    imp-null  lsr: 10.132.0.1:0
  10.12.0.0/24
        in label:     17
        out label:    imp-null  lsr: 10.132.0.1:0
  10.132.0.1/32
        out label:    imp-null  lsr: 10.132.0.1:0
  10.134.0.2/32
        in label:     18
        out label:    16        lsr: 10.132.0.1:0
  10.134.0.4/32
        in label:     19
        out label:    17        lsr: 10.132.0.1:0
  10.138.0.1/32
        out label:    imp-null  lsr: 10.132.0.1:0
```

Cisco 10000 Series Examples Only

The following sample shows binding information for a Cisco 10000 series router:

```
Router# show mpls ip binding

  0.0.0.0/0
        in label:     imp-null
  10.29.0.0/16
        in label:     imp-null
        out label:    imp-null  lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0
  10.20.0.0/24
        in label:     imp-null
        out label:    26        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0
```

```
  10.30.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.66.66.66:0
        out label:    18        lsr: 10.44.44.44:0
  10.44.44.44/32
        in label:     21
        out label:    19        lsr: 10.66.66.66:0
        in label:     imp-null
        out label:    26        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0
  10.30.0.0/24
        in label:     imp-null
        out label:    imp-null  lsr: 10.66.66.66:0
        out label:    18        lsr: 10.44.44.44:0
  10.44.44.44/32
        in label:     21
        out label:    19        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0    inuse
  10.55.55.55/32
        in label:     imp-null
        out label:    25        lsr: 10.66.66.66:0
        out label:    55        lsr: 10.44.44.44:0
  10.66.66.66/32
        in label:     18
        out label:    imp-null  lsr: 10.66.66.66:0    inuse
        out label:    16        lsr: 10.44.44.44:0
  10.255.254.244/32
        in label:     24
        out label:    16        lsr: 10.66.66.66:0
        out label:    59        lsr: 10.44.44.44:0
```

In the following example on a Cisco 10000 series router, a request is made for the display of the label binding information for prefix 172.16.44.44/32:

```
Router# show mpls ip binding 172.16.44.44 32

  172.16.44.44/32
        in label:     21
        out label:    19        lsr: 10.66.66.66:0
        out label:    imp-null  lsr: 10.44.44.44:0    inuse
```

In the following example on a Cisco 10000 series router, the **local-label** keyword is used to request that label binding information be displayed for the prefix with local label 21:

```
Router# show mpls ip binding local-label 21

  10.44.44.44/32
        in label:     21
```

Table 96 describes the significant fields shown in the displays.

Table 96 show mpls ip binding Field Descriptions

Field	Description
172.16.44.44/32	Destination prefix. Indicates that the following lines are for a particular destination (network/mask).
in label	Incoming label. This is the local label assigned by the label switch router (LSR) and advertised to other LSRs. The label value imp-null indicates the well-known Implicit NULL label.

Table 96 show mpls ip binding Field Descriptions (continued)

Field	Description
out label	Outgoing label. This is a remote label learned from an LDP neighbor. The neighbor is identified by its LDP ID in the lsr field.
inuse	Indicates that the outgoing label is in use for Multiprotocol Label Switching (MPLS) forwarding, that is, it is installed in the MPLS forwarding table (the Label Forwarding Information Base [LFIB]).
in vc label	Incoming MPLS ATM label. This is the local VPI/VCI assigned by the LSR as the incoming label for the destination and advertised to the upstream LSRs. **Note** This field applies to the Cisco 7500 series routers only.
out vc label	Outgoing MPLS ATM label. This is the VPI/VCI learned from the destination next hop as its label for the destination and advertised to this LSR. **Note** This field applies to the Cisco 7500 series routers only.
ATM1/0.8	The ATM interface with which the MPLS ATM label is associated. **Note** This field applies to the Cisco 7500 series routers only.
Active	State of the label VC (LVC) associated with the destination prefix. **Note** This field applies to the Cisco 7500 series routers only. States are the following: • Active. Established and operational. • Bindwait. Waiting for a response from the destination next hop. • Remote Resource Wait. Waiting for resources (VPI/VCI) to become available on the destination next hop. • Parent Wait. Transit LVC upstream side waiting for downstream side to become active. • AbortAckWait. Waiting for response to a Label Abort message sent to the destination next hop. • ReleaseWait. Waiting for response to a Label Withdraw message sent to an upstream neighbor.

Table 96 show mpls ip binding Field Descriptions (continued)

Field	Description
vcd 49	Virtual circuit descriptor number for the LVC. **Note** This field applies to the Cisco 7500 series routers only.
ingress 3 hops	Indicates whether the LSR is an ingress, transit, or egress node for the destination. **Note** This field applies to the Cisco 7500 series routers only. Options include the following: • Ingress 3 hops. The LSR is an ingress edge router for the MPLS ATM cloud for the destination. • Egress. The LSR is an egress edge router for the MPLS ATM cloud for the destination. • Transit. The LSR is a transit LSR within the MPLS ATM cloud for the destination.

The following sample output displays detailed information about the label bindings:

```
Router# show mpls ip binding detail

  10.0.0.0/8, rev 2, chkpt: add-skipped
        in label:     imp-null   (owner LDP)
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    imp-null  lsr: 10.60.60.60:0
        out label:    imp-null  lsr: 10.30.30.30:0
  10.10.10.10/32, rev 18, chkpt: added
        in label:     17         (owner LDP)
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    142       lsr: 10.60.60.60:0
        out label:    19        lsr: 10.30.30.30:0    inuse
  10.0.0.1/32, rev 10, chkpt: add-skipped
        in label:     imp-null   (owner LDP)
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    21        lsr: 10.60.60.60:0
        out label:    17        lsr: 10.30.30.30:0
  10.30.30.30/32, rev 20, chkpt: added
        in label:     18         (owner LDP)
          Advertised to:
          10.60.60.60:0          10.30.30.30:0
        out label:    22        lsr: 10.60.60.60:0
```

Table 97 describes the significant fields shown in the display.

Table 97 show mpls ip binding detail Field Descriptions

Field	Description
chkpt	The status of the checkpointed entry. • add-skipped—Means that the local label is a null label and does not need to be checkpointed. • added— Means that the checkpoints entry was copied to the backup Route Processor (RP)
owner	The application that created the binding. • owner LDP—Means that LDP created the binding. • owner other—Means that another application created the binding, possibly Border Gateway protocol (BGP).
Advertised to	The LSRs that received the local label binding.
inuse or stale	The status of the label. • inuse—Indicates that the outgoing label is in use for MPLS forwarding, that is, it is installed in the MPLS forwarding table (LFIB). • stale—Indicates a label that is no longer in use. This happens when an LDP session is lost and the routers begin a graceful restart. Then the remote label bindings are marked stale.

Cisco 7500 Series Example Only

The following sample output shows summary information about the label bindings learned by LDP:

```
Router# show mpls ip binding summary

Total number of prefixes: 53

Generic label bindings
                     assigned        learned
       prefixes      in labels     out labels
             53             53             51

ATM label bindings summary
      interface   total  active   local  remote   Bwait   Rwait  IFwait
       ATM1/0.8      47      47      40       7       0       0       0
Router#
```

Table 98 describes the significant fields shown in the display.

Table 98 show mpls ip binding summary Field Descriptions (Cisco 7500 Series Example)

Field	Description
Total number of prefixes	Number of destinations for which the LSR has label bindings.
Generic label bindings	Indicates the start of summary information for “generic” label bindings. Generic labels are used for MPLS forwarding on all interface types except MPLS ATM interfaces.
prefixes	Number of destinations for which the LSR has a generic label binding.

Table 98 show mpls ip binding summary Field Descriptions (Cisco 7500 Series Example)

assigned in labels	Number of prefixes for which the LSR has assigned an incoming (local) label.
learned out labels	Number of prefixes for which the LSR has learned an outgoing (remote) label from an LDP neighbor.
ATM label bindings summary	Indicates the start of summary information for MPLS ATM label bindings. An ATM label is a VPI/VCI.
interface	Indicates a row in the ATM label bindings summary table. The summary information in the row is for ATM labels associated with this interface.
total	Total number of ATM labels associated with the interface.
active	Number of ATM labels (LVCs) in the active (operational) state.
local	Number of ATM labels assigned by this LSR for the interfaces. These are incoming labels.
remote	Number of ATM labels learned from the neighbor LSR for this interface. These are outgoing labels.
Bwait	Number of bindings (LVCs) waiting for a label assignment from the neighbor LSR for the interface.
Rwait	Number of bindings (LVCs) waiting for resources (VPI/VCIs) to become available on the neighbor LSR for the interface.
IFwait	Number of bindings (LVCs) waiting for labels to be installed for switching use.

Cisco 10000 Series Example Only

The following sample output displays summary information about the label bindings learned by LDP:

```
Router# show mpls ip binding summary

Total number of prefixes: 53

Generic label bindings
                     assigned        learned
       prefixes      in labels     out labels
             53             53             51
```

Table 99 describes the significant fields shown in the display.

Table 99 show mpls ip binding summary Field Descriptions (Cisco 10000 Series Example)

Field	Description
Total number of prefixes	Number of destinations for which the LSR has label bindings.
Generic label bindings	Indicates the start of summary information for “generic” label bindings. Generic labels are used for MPLS forwarding on all interface types except MPLS ATM interfaces.
prefixes	Number of destinations for which the LSR has a generic label binding.

Table 99 show mpls ip binding summary Field Descriptions (Cisco 10000 Series Example)

Field	Description
assigned in labels	Number of prefixes for which the LSR has assigned an incoming (local) label.
learned out labels	Number of prefixes for which the LSR has learned an outgoing (remote) label from an LDP neighbor.

Related Commands

Command	Description
show mpls atm-ldp bindings	Displays specified entries from the ATM label binding database.
show mpls ldp bindings	Displays the contents of the LIB.

show mpls ip iprm counters

To display the number of occurrences of various Multiprotocol Label Switching (MPLS) IP Rewrite Manager (IPRM) events, use the **show mpls ip iprm counters** command in privileged EXEC mode.

show mpls ip iprm counters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command reports the occurrences of IPRM events.

Examples

The command in the following example displays the events that the IPRM logs:

```
Router# show mpls ip iprm counters

  CEF Tree Changes Processed/Ignored:           91/12
  CEF Deletes Processed/Ignored:                12/2
  Label Discoveries:                            74
  Rewrite Create Successes/Failures:            60/0
  Rewrite Gets/Deletes:                         82/0
  Label Announcements: Info/Local/Path:         6/119/80
  Walks: Recursion Tree/CEF Full/CEF interface: 78/2/0
```

Table 100 describes the significant fields shown in the display.

Table 100 show mpls ip iprm counters Command Field Descriptions

Field	Description
CEF Tree Changes Processed/Ignored	Processed—The number of Cisco Express Forwarding tree change announcements that IPRM processed. Ignored—The number of Cisco Express Forwarding tree change announcements that IPRM ignored. Typically, IPRM processes tree change announcements only for prefixes in a routing table.
CEF Deletes Processed/Ignored	Processed—The number of Cisco Express Forwarding delete entry announcements that IPRM processed. Ignored—The number of Cisco Express Forwarding delete entry announcements that IPRM ignored. Typically, IPRM processes delete entry announcements only for prefixes in a routing table.
Label Discoveries	The number of label discoveries performed by IPRM. Label discovery is the process by which IPRM obtains prefix labels from the IP Label Distribution Modules (LDMs).
Rewrite Create Successes/Failures	Successes—The number of times IPRM successfully updated the MPLS forwarding information. Failures—The number of times IPRM attempted to update the MPLS forwarding information and failed.
Rewrite Gets/Deletes	Gets—The number of times IPRM retrieved forwarding information from the MPLS forwarding infrastructure. Deletes—The number of times IPRM removed prefix forwarding information from the MPLS forwarding infrastructure.

Table 100 show mpls ip iprm counters Command Field Descriptions (continued)

Field	Description
CEF Tree Changes Processed/Ignored	Processed—The number of Cisco Express Forwarding tree change announcements that IPRM processed. Ignored—The number of Cisco Express Forwarding tree change announcements that IPRM ignored. Typically, IPRM processes tree change announcements only for prefixes in a routing table.
Label Announcements: Info/Local/Path	Info—The number of times an IP label distribution module informed IPRM that label information for a prefix changed. Local—The number of times an IP label distribution module specified local labels for a prefix. Path—The number of times an IP LDM specified outgoing labels for a prefix route.
Walks: Recursion Tree/CEF Full/CEF interface	Recursion Tree—The number of times IPRM requested Cisco Express Forwarding to walk the recursion (path) tree for a prefix. CEF Full—The number of times IPRM requested Cisco Express Forwarding to walk a Cisco Express Forwarding table and notify IPRM about each prefix. CEF interface—The number of times IPRM requested Cisco Express Forwarding to walk a Cisco Express Forwarding table and notify IPRM about each prefix with a path that uses a specific interface.

Related Commands

Command	Description
clear mpls ip iprm counters	Clears the IPRM counters.
show mpls ip iprm ldm	Displays information about the IP LDMs that have registered with the IPRM.

show mpls ip iprm ldm

To display information about the IP Label Distribution Modules (LDMs) that have registered with the IP Rewrite Manager (IPRM), use the **show mpls ip iprm ldm** command in privileged EXEC mode.

show mpls ip iprm ldm [**table** {**all** | *table-id*} | **vrf** *vrf-name*] [**ipv4** | **ipv6**]

Cisco 10000 Series Routers

show mpls ip iprm ldm [**table** {**all** | *table-id*} | **vrf** *vrf-name*] [**ipv4**]

Syntax Description

table	(Optional) Displays the LDMs for one or more routing tables.
all	Displays the LDMs for all routing tables.
table-id	Displays the LDMs for the routing table you specify. Table 0 is the default or global routing table.
vrf	(Optional) Displays the LDMs for the VPN routing and forwarding (VRF) instance you specify.
vrf-name	(Optional) The name of the VRF instance. You can find VRF names with the **show ip vrf** command.
ipv4	(Optional) Displays IPv4 LDMs.
ipv6	(Optional) Displays IPv6 LDMs. **Note** Applies to Cisco 7500 series routers only.

Defaults

If you do not specify any keywords or parameters, the command displays the LDMs for the global routing table (the default).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SSH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command displays the IP LDMs registered with IPRM.

Examples

The command in the following example displays the LDMs for the global routing tables. It shows that two LDMs (lcatm and ldp) are registered for the ipv4 global routing table, and that one LDM (bgp ipv6) is registered for the ipv6 global routing table.

```
Router# show mpls ip iprm ldm

  table (glbl;ipv4); ldms: 2
    lcatm, ldp
  table (glbl;ipv6); ldms: 1
    bgp ipv6
```

The command in the following example displays all of the LDMs registered with IPRM. The output shows the following:

- The LDMs called lcatm and ldp have registered with IPRM for the ipv4 global table.
- The LDM called bgp ipv6 is registered for the IPv6 global table.
- The LDM called bgp vpnv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all

  table (glbl;ipv4); ldms: 2
    lcatm, ldp
  table (glbl;ipv6); ldms: 1
    bgp ipv6
  table (all-tbls;ipv4); ldms: 1
    bgp vpnv4
```

The command in the following example displays the LDMs registered for the IPv6 routing tables.

```
Router# show mpls ip iprm ldm ipv6

  table (glbl;ipv6); ldms: 1
    bgp ipv6
```

Cisco 10000 Series Examples Only

The command in the following example displays the LDMs for the global routing tables. It shows that one LDM (ldp) is registered for the ipv4 global routing table.

```
Router# show mpls ip iprm ldm

  table (glbl;ipv4); ldms: 1
    ldp
```

The command in the following example displays all of the LDMs registered with IPRM. The output shows the following:

- The LDM called ldp has registered with IPRM for the ipv4 global table.
- The LDM called bgp vpnv4 is registered for all IPv4 vrf routing tables.

```
Router# show mpls ip iprm ldm table all

  table (glbl;ipv4); ldms: 1
    ldp
  table (all-tbls;ipv4); ldms: 1
    bgp vpnv4
```

Related Commands

Command	Description
show mpls ip iprm counters	Displays the number of occurrences of various IPRM events.

show mpls l2 vc detail

To display detailed information related to the virtual connection (VC), use the **show mpls l2 vc detail** command in user EXEC or privileged EXEC mode.

show mpls l2 vc *vc-id* **detail**

Syntax Description

vc-id	Name of the VC.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. STANDBY and HOTSTANDBY were added as options for the Status column in output displays.

Examples

This example shows how to display detailed status for a specific VC:

```
Router# show mpls l2 vc 1100 detail

Local interface: VFI VPLS-1100 up
 MPLS VC type is VFI, internetworking type is Ethernet
 Destination address: 1.1.1.1,VC ID:1100, VC status: up
  Output interface: Tu0,imposed label stack {27 17}
  Preferred path: not configured
  Default path: active
  Next hop:point2point
 Create time:2d23h, last status change time: 2d23h
 Signaling protocol: LDP, peer 1.1.1.1:0 up
  MPLS VC labels: local 17, remote 17
  Group ID: local 0, remote 0
  MTU: local 1500, remote 1500
  Remote interface description:
 Sequencing: receive disabled, send disabled
 VC statistics
  packet totals: receive 1146978, send 3856011
  byte totals: receive 86579172, send 316899920
  packet drops: receive 0, send 0
```

The following examples show the status of the active and backup pseudowires before, during, and after a switchover.

The **show mpls l2 vc detail** command on the active PE router displays the status of the pseudowires.

```
Router# show mpls l2 vc detail
```

```
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        UP
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        STANDBY
```

The **show mpls l2 vc detail** command on the backup PE router displays the status of the pseudowires. The active pseudowire on the backup PE router has the HOTSTANDBY status.

```
Router-standby# show mpls l2 vc detail

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        HOTSTANDBY
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        DOWN
```

During a switchover, the status of the active and backup pseudowires changes:

```
Router# show mpls l2 vc detail

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        RECOVERING
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        DOWN
```

After the switchover is complete, the recovering pseudowire shows a status of UP:

```
Router# show mpls l2 vc detail

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0.1      ATM VPC CELL 50            10.1.1.2         100        UP
AT0/2/0.1      ATM VPC CELL 50            10.1.1.3         100        STANDBY
```

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show mpls l2transport binding

To display virtual circuit (VC) label binding information, use the **show mpls l2transport binding** command in EXEC mode.

show mpls l2transport binding [*vc-id* | *ip-address* | **local-label** *number* | **remote-label** *number*}

Syntax Description

vc-id	(Optional) Displays VC label binding information for the specified VC.
ip-address	(Optional) Displays VC label binding information for the specified VC destination.
local-label *number*	(Optional) Displays VC label binding information for the specified local assigned label.
remote-label *number*	(Optional) Displays VC label binding information for the specified remote assigned label.

Command Modes

EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(27)S	This command was updated to display AToM Virtual Circuit Connection Verification (VCCV) information.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(30)S	This command was updated to display Connectivity Verification (CV) type capabilities.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was updated to display Circuit Emulation (CEM) information for the Cisco 7600 series router.
Cisco IOS XE Release 2.3	The command was updated to display information about multisegment pseudowires.
12.2(1)SRE	This command was modified to display VC label binding information for the control word.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Examples

The following example shows the VC label binding information for Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later releases:

```
Router# show mpls l2transport binding

Destination Address: 10.0.0.203,  VC ID: 1
    Local Label:  16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
```

```
        VCCV Capabilities: Type 1, Type 2
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV Capabilities: Type 1, Type 2
```

The following examples shows the VC label binding information for Cisco IOS Release 12.2(30)S and later releases:

```
Router# show mpls l2transport binding

Destination Address: 10.5.5.51,  VC ID: 108
    Local Label:  16
        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: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
```

The output of the command changed between Cisco IOS releases. The following table maps the older output to the new output:

Output in Cisco IOS Releases 12.0(27)S and 12.2(18)SXE	Output In Cisco IOS Release 12.2(30)S
VCCV Capabilities	VCCV: CC Type
Type 1	CW [1]
Type 2	RA [2]

The following example is a sample output of the **show mpls l2transport binding** command that shows the VC label binding information on a Cisco uBR10012 router:

```
Router# show mpls l2transport binding

Destination Address: 10.76.1.1,  VC ID: 2002
  Local Label:  42
      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: 60
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2003
  Local Label:  46
      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: 27
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2004
  Local Label:  unassigned.
  Remote Label: 111
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
```

```
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2017
  Local Label:  43
      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: 110
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2018
  Local Label:  45
      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: 88
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
Destination Address: 10.76.1.1,  VC ID: 2019
  Local Label:  44
      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: 16
      Cbit: 1,    VC Type: Ethernet,    GroupID: 0
      MTU: 1500,   Interface Desc: n/a
      VCCV: CC Type: RA [2]
            CV Type: LSPV [2]
```

Table 101 describes the significant fields shown in the display.

Table 101 show mpls l2transport binding Field Descriptions

Field	Description
Destination Address	The IP address of the remote router's interface that is at the other end of the VC.
VC ID	The virtual circuit identifier assigned to one of the interfaces on the router.
Local Label	The VC label that a router signals to its peer router, which is used by the peer router during imposition.
Remote Label	The disposition VC label of the remote peer router.
Cbit	The control word bit. If it is set, the value is 1.
VC Type	The type of VC, such as Frame Relay, Ethernet, and ATM.
GroupID	The group ID assigned to the local or remote VCs.
MTU	The maximum transmission unit assigned.
Interface Desc	Interface parameters, if applicable.

Table 101 show mpls l2transport binding Field Descriptions (continued)

Field	Description
VCCV Capabilities	(Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later releses) AToM VCCV information. This field displays how an AToM VCCV packet is identified. • Type 1—The Protocol ID field of the AToM Control Word (CW) is identified in the AToM VCCV packet. • Type 2—An MPLS Router Alert (RA) Level above the VC label in identified in the AToM VCCV packet. Type 2 is used for VC types that do not support or do not interpret the AToM Control Word.
VCCV: CC Type	(Cisco IOS Releases 12.2(30)S and later releases) The types of Control Channel (CC) processing that are supported. The number indicates the position of the bit that was set in the received octet. The following values can be displayed: • CW [1]—Control Word • RA [2]—Router Alert • TTL [3]—Time to Live • Unkn [*x*]—Unknown
CV Type	(Cisco IOS Releases 12.2(30)S and later releases) The type of Connectivity Verification (CV) packets that can be processed in the control channel of the MPLS pseudowire. The number indicates the position of the bit that was set in the received octet. • ICMP [1]—Internet Control Management Protocol (ICMP) is used to verify connectivity. • LSPV [2]—LSP Ping is used to verify connectivity. • BFD [3]—Bidirectional Forwarding Detection is used to verify connectivity for more than one pseudowire. • Unkn [*x*]—A CV type was received that could not be interpreted.

The following sample output shows information about L2VPN multisegment pseudowires (in bold):

```
Router# show mpls l2transport binding

  Destination Address: 10.1.1.1,  VC ID: 102
    Local Label:  17
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
        PW Switching Point:
             Vcid   local IP addr      remote IP addr      Description
101         10.11.11.11    10.20.20.20         PW Switching Point PE3
              100         10.20.20.20    10.11.11.11         PW Switching Point PE2
```

Table 102 describes the significant fields shown in the display.

Table 102 show mpls l2transport binding Field Descriptions for Multisegment Pseudowires

Field	Description
TTL	The Time to Live (TTL) setting of the label.
Vcid	The virtual circuit identifier.
local IP addr	The local IP address assigned to the switching point.
remote IP addr	The remote IP address assigned to the switching point.
Description	The description assigned to the switching point.

CEM circuits are supported on the Cisco 7600 series router transport time-division multiplexing (TDM) traffic. The following example displays AToM VCs and the applicable local and remote CEM settings as exchanged over LDP label mapping messages.

```
Router# show mpls l2transport binding

  Destination Address: 10.7.1.1,  VC ID: 100
    Local Label:  18
        Cbit: 1,    VC Type: CESoPSN BRI,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
        CEM/TDM Options
              Payload Bytes: 80,    Payload Type: 0
              SP bits: 11 - Data/Signaling,    CAS Type: CAS T1 SF
              RTP header in use: Yes,    Bitrate (Kbit/s): 64
              Differential Timestamp Mode: disabled
              Clock Frequency (kHz): 64
              Synchronization Source id: 0
    Remote Label: 19
        Cbit: 1,    VC Type: CESoPSN BRI,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
        CEM/TDM Options
              Payload Bytes: 80,    Payload Type: 0
              SP bits: 11 - Data/Signaling,    CAS Type: CAS T1 SF
              RTP header in use: Yes,    Bitrate (Kbit/s): 64
```

```
            Differential Timestamp Mode: disabled
            Clock Frequency (kHz): 64
            Synchronization Source id: 0
```

The following example shows the VC label binding information for the control word, which in this case is set to 0, meaning that it is disabled:

```
Router# show mpls l2transport binding 102

Destination Address: 10.1.1.3,  VC ID: 102
    Local Label:  1004
        Cbit: 0,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 1005
        Cbit: 0,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
```

The following example shows the maximum number of cells that can be packed (in bold) for both provider edge routers, as specified by the **cell-packing** command:

```
Router# show mpls l2transport binding 1010
  Destination Address: 10.6.1.2,  VC ID: 1010
    Local Label:  20008
        Cbit: 1,    VC Type: ATM VCC CELL,    GroupID: 0
        MTU: n/a,   Interface Desc: n/a
        Max Concatenated ATM Cells: 10
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2], BFD [3]
    Remote Label: 47
        Cbit: 1,    VC Type: ATM VCC CELL,    GroupID: 0
        MTU: n/a,   Interface Desc: n/a
        Max Concatenated ATM Cells: 10
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
```

Related Commands

Command	Description
show mpls l2transport hw-capability	Displays the transport types and their supported capabilities.
show mpls l2transport vc	Displays information about AToM VCs and static pseudowires that have been enabled to route Layer 2 packets on a router.

show mpls l2transport checkpoint

To display checkpointing information about Any Transport over MPLS (AToM) virtual circuits (VCs), use the **show mpls l2transport checkpoint** command in privileged EXEC mode.

show mpls l2transport checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Examples

The output of the commands varies, depending on whether the output reflects the active or standby Route Processor (RP).

On the active RP, the command displays the following output:

```
Router# show mpls l2transport checkpoint

AToM Checkpoint info for active RP
Checkpointing is allowed
Bulk-sync checkpointed state for 1 VC
```

On the standby RP, the command displays the following output:

```
Router# show mpls l2transport checkpoint

AToM HA Checkpoint info for standby RP
1 checkpoint information block in use
```

In general, the output on the active RP shows that checkpointing information was sent to the backup RP. The output on the backup RP shows that checkpointing information was received from the active RP.

Related Commands

Command	Description
show mpls l2transport vc	Displays information about the checkpointed data when checkpointing is enabled.

show mpls l2transport hw-capability

To display the transport types supported on an interface, use the **show mpls l2transport hw-capability** command in privileged EXEC mode.

show mpls l2transport hw-capability interface *type number*

Syntax Description

interface	Displays information for the specified interface.
type number	Type and number of the interface. For example, serial6/0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(27)S	This command was updated to display AToM Virtual Circuit Connection Verification (VCCV) information.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(30)S	This command was updated to display VCCV type capabilities.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

This command can help you determine the interface to use for the various transport types. Use this command to check if core-facing and edge-facing interfaces can accommodate different transport types.

Examples

The following is partial sample output of the **show mpls l2transport hw-capability** command for Cisco IOS Releases 12.0(23)S, 12.2(14)S, and 12.2(15)T and later. For more information on the fields, see Table 103.

```
Router# show mpls l2transport hw-capability interface serial5/1

Interface Serial5/1

Transport type FR DLCI
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
  Edge functionality:
    MPLS label imposition supported
    Control word processing supported
    Sequence number processing not supported
.
.
```

.

Note These examples show only a portion of the output. The command displays the the capabilities of every transport type.

The following is partial sample output of the **show mpls l2transport hw-capability** command for Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later releases. This output shows VCCV data under the Core Functionality section. Type 1 means that the AToM Control Word identified the AToM VCCV packet. For more information on the fields, see Table 103.

```
Transport type FR DLCI
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type 1 processing supported

  Edge functionality:
    MPLS label imposition supported
    Control word processing supported
    Sequence number processing not supported
```

.

The following is partial sample output of the **show mpls l2transport hw-capability** command for Cisco IOS Releases 12.2(30)S and later releases. The VCCV output shows that AToM Control Word (CW) identified the AToM VCCV packet. For more information on the fields, see Table 103.

```
Transport type FR DLCI
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type CW [1] processing supported

  Edge functionality:
    MPLS label imposition supported
    Control word processing supported
    Sequence number processing not supported
```

.

The following is a sample output of the **show mpls l2transport hw-capability** command that displays the transport types supported on the Gigabit Ethernet interface 3/0/0 on a Cisco uBR10012 router:

```
Router# show mpls l2transport hw-capability interface gigabitethernet 3/0/0

Interface GigabitEthernet3/0/0

Transport type DOCSIS
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type CW [1] processing not supported
  Edge functionality:
    Not supported
```

```
Transport type DOCSIS VLAN
  Core functionality:
    MPLS label disposition supported
    Control word processing supported
    Sequence number processing not supported
    VCCV CC Type CW [1] processing not supported
  Edge functionality:
    Not supported
```

The output of the command changed between Cisco IOS releases. The following table maps the older output to the newer output:

Output in Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later	Output In Cisco IOS Release 12.2(30)S
`VCCV CC processing supported`	`VCCV CC processing supported`
`Type 1`	`Type CW [1]`

Table 103 describes the fields shown in the **show mpls l2transport hw-capability** command display.

Table 103 show mpls l2transport hw-capability Field Descriptions

Field	Description
Transport type	Indicates the transport type.
Core functionality	Displays the functionalities that the core-facing interfaces support, such as label disposition, and control word and sequence number processing.
VCCV CC Type processing supported	Displays whether the core-facing interfaces support Control Word processing, or Router Alert Processing. (Cisco IOS Releases 12.0(27)S and 12.2(18)SXE and later) • Type 1—The Protocol ID field of in the AToM Control Word (CW) identified the AToM VCCV packet. (Cisco IOS Releases 12.2(30)S and later) • CW [1]—Control Word • Unkn [*x*]—Unknown. The number indicates the position of the bit that was set in the received octet.
Edge functionality	Displays the functionalities that the edge-facing interfaces support, such as label disposition, and control word and sequence number processing.

Related Commands

Command	Description
show mpls l2transport binding	Displays virtual circuit (VC) label binding information.
show mpls l2transport checkpoint	Displays the checkpoint information about Any Transport over MPLS (AToM) virtual circuits.
show mpls l2transport summary	Displays summary information about virtual circuits.
show mpls l2transport vc	Displays information about AToM virtual circuits and static pseudowires that have been enabled to route Layer 2 packets on a router.

show mpls l2transport summary

To display summary information about virtual circuits (VCs) that have been enabled to route Any Transport over MPLS (AToM) Layer 2 packets on a router, use the **show mpls l2transport summary** command in privileged EXEC mode.

show mpls l2transport summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Examples

The following is a sample output of the **show mpls l2transport summary** command that shows summary information about the VCs that have been enabled to transport Layer 2 packets:

```
Router# show mpls l2transport summary

Destination address: 10.16.24.12 Total number of VCs: 60
0 unknown, 58 up, 0 down, 2 admin down
5 active vc on MPLS interface PO4/0
```

The following is a sample output of the **show mpls l2transport summary** command that shows summary information about the VCs that have been enabled to transport Layer 2 packets on a Cisco uBR10012 router:

```
Router# show mpls l2transport summary

Destination address: 10.76.1.1, total number of vc: 6
  0 unknown, 5 up, 1 down, 0 admin down, 0 recovering, 0 standby
  5 active vc on MPLS interface Gi3/0/0
```

Table 104 describes the fields shown in the **show mpls l2transport summary** command display.

Table 104 show mpls l2transport summary Field Descriptions

Field	Description
Destination address	IP address of the remote router to which the VC has been established.
Total number of VCs	Number of VCs that have been established.
unknown	Number of VCs that are in an unknown state.
up	Number of VCs that are operational.
down	Number of VCs that are not operational.
admin down	Number of VCs that have been disabled.

Related Commands

Command	Description
show mpls l2transport binding	Displays virtual circuit (VC) label binding information.
show mpls l2transport checkpoint	Displays the checkpoint information about Any Transport over MPLS (AToM) virtual circuits.
show mpls l2transport hw-capability	Displays the transport types and their supported capabilities.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

show mpls l2transport vc

To display information about Any Transport over MPLS (AToM) virtual circuits (VCs) and static pseudowires that have been enabled to route Layer 2 packets on a router, use the **show mpls l2transport vc** command in user EXEC or privileged EXEC mode.

show mpls l2transport vc [[**vcid** *vc-id-min* | *vc-id-min*] [*vc-id-max*]] [**interface** *type number* [*local-circuit-id*]] [**destination** {*ip-address* | *host-name*}] [**detail**]

Syntax Description

vcid	(Optional) Specifies the VC ID.
vc-id-min	(Optional) Minimum VC ID value. The range is from 1 to 4294967295.
vc-id-max	(Optional) Maximum VC ID value. The range is from 1 to 4294967295.
interface	(Optional) Specifies the interface or subinterface of the router that has been enabled to transport Layer 2 packets. Use this keyword to display information about the VCs that have been assigned VC IDs on that interface or subinterface.
type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
local-circuit-id	(Optional) The number assigned to the local circuit. This argument value is supported only with the following transport types: • For Frame Relay, enter the data-link connection identifier (DLCI) of the permanent virtual circuit (PVC). • For ATM adaptation layer 5 (AAL5) and cell relay, enter the virtual path identifier (VPI) or virtual channel identifier (VCI) of the PVC. • For Ethernet VLANs, enter the VLAN number.
destination	(Optional) Specifies the remote router.
ip-address	(Optional) The IP address of the remote router.
host-name	(Optional) The name assigned to the remote router.
detail	(Optional) Specifies the detailed information about the VCs.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(8a)E	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.

Release	Modification
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S and implemented on the Cisco 10720 router.
12.0(23)S	This command was modified. The **interface** and **destination** keywords were added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and was implemented on the Supervisor Engine 720.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and was implemented on the Cisco 10000 series routers. Example output was changed for the Cisco 10000 series router, and two fields (SSO Descriptor and SSM segment/switch IDs) were removed from the output, because they are not supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was updated to include forwarding equivalence class (FEC) 129 signaling information for pseudowires that are configured through VPLS Autodiscovery, and to support provisioning Any Transport over MPLS (AToM) static pseudowires.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was modified. This command was updated to display the number of MAC address withdrawal messages sent and received as part of the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature. This command was updated to display pseudowire status between peer routers that have been configured for the MPLS Pseudowire Status Signaling feature.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.
Cisco IOS XE Release 2.3	This command was modified. This command output was updated to display the following information: • The status of pseudowires before, during, and after a switchover. • The status of a pseudowire switching point for multisegment pseudowires. • The number of packets and bytes being sent from the router. The VC statistics fields include the word “transit” to show that the packet totals no longer include packets being sent to the router.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

If you do not specify any keywords or arguments, the command displays a summary of all the VCs.

Examples

The output of the commands varies, depending on the type of Layer 2 packets being transported over the AToM VCs.

The following sample output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router:

```
Router# show mpls l2transport vc

Local intf     Local circuit      Dest address    VC ID      Status
-------------  ------------------ --------------- ---------- ----------
Se5/0          FR DLCI 55         10.0.0.1        55         UP
AT4/0          ATM AAL5 0/100     10.0.0.1        100        UP
AT4/0          ATM AAL5 0/200     10.0.0.1        200        UP
AT4/0.300      ATM AAL5 0/300     10.0.0.1        300        UP
```

Table 105 describes the fields shown in the display.

Table 105 show mpls l2transport vc Field Descriptions

Field	Description
Local intf	The interface on the local router that has been enabled to transport Layer 2 packets.
Local circuit	The type and number (if applicable) of the local circuit. The output shown in this column varies, depending on the transport type: • For Frame Relay, the output shows the DLCI of the PVC. • For ATM cell relay and AAL5, the output shows the VPI or VCI of the PVC. • For Ethernet VLANs, the output shows the VLAN number. • For PPP and High-Level Data Link Control (HDLC), the output shows the interface number.
Dest address	The IP address of the remote router's interface that is the other end of the VC.
VC ID	The virtual circuit identifier assigned to one of the interfaces on the router.
Status	The status of the VC. The status can be one of the following: • ADMIN DOWN—The VC has been disabled by a user. • DOWN—The VC is not ready to carry traffic between the two VC endpoints. Use the **detail** keyword to determine the reason that the VC is down. • HOTSTANDBY—The active pseudowire on a standby route processor. • RECOVERING—The VC is recovering from a stateful switchover. • STANDBY—The VC is designated as the backup circuit in a stateful switchover configuration. • UP—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed. – The disposition interface is programmed if the VC has been configured and the client interface is up. – The imposition interface is programmed if the disposition interface is programmed and you have a remote VC label and an Interior Gateway Protocol (IGP) label. The IGP label can be implicit null in a back-to-back configuration. An IGP label means there is a label switched path (LSP) to the peer.

The following example shows information about the NSF, SSO, and graceful restart capability. The SSO portion indicates when checkpointing data has either been sent (on active) or received (on standby). When SSO data has not been successfully sent or has been released, the SSO information is not shown.

```
Router# show mpls l2transport vc detail

Local interface: Fa5/1/1.2 down, line protocol down, Eth VLAN 2 up
  Destination address: 10.55.55.2, VC ID: 1002, VC status: down
    Output interface: Se4/0/3, imposed label stack {16}
    Preferred path: not configured
Default path: active
    Tunnel label: imp-null, next hop point2point
  Create time: 02:03:29, last status change time: 02:03:26
  Signaling protocol: LDP, peer 10.55.55.2:0 down
    MPLS VC labels: local 16, remote unassigned
    Group ID: local 0, remote unknown
    MTU: local 1500, remote unknown
    Remote interface description:
  Sequencing: receive disabled, send disabled
  SSO Descriptor: 10.55.55.2/1002, local label: 16
    SSM segment/switch IDs: 12290/8193, PWID: 8193
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

Table 105 to Table 109 describes the fields shown in the display.

The following example shows information provided when an AToM static pseudowire has been provisioned and the **show mpls l2transport vc detail** command is used to check the configuration. The Signaling protocol field specifies Manual, because a directed control protocol such as Label Distribution Protocol (LDP) cannot be used to exchange parameters on static pseudowires. The remote interface description field seen for nonstatic pseudowire configurations is not displayed, because remote information is exchanged using signaling between the PE routers and this is not done on static pseudowires.

```
Router# show mpls l2transport vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
   Destination address: 10.1.1.2, VC ID: 100, VC status: up
     Output interface: Et2/0, imposed label stack {10003 150}
     Preferred path: not configured
     Default path: active
     Next hop: 10.0.0.2
   Create time: 00:18:57, last status change time: 00:16:10
   Signaling protocol: Manual
     MPLS VC labels: local 100, remote 150
     Group ID: local 0, remote 0
     MTU: local 1500, remote 1500
     Remote interface description:
   Sequencing: receive disabled, send disabled
   VC statistics:
     packet totals: receive 219, send 220
     byte totals:   receive 20896, send 26694
     packet drops:  receive 0, send 0
```

Table 105 to Table 109 describes the fields shown in the display.

The following example shows the VC statistics displaying the number of packets and bytes being sent from the router. The VC statistics fields include the word “transit” to show that the packet totals no longer include packets being sent to the router.

```
Router# show mpls l2transport vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
.
.
.
VC statistics:
     transit packet totals: receive 219, send 220
     transit byte totals:   receive 20896, send 26694
     transit packet drops:  receive 0, send 0
```

Table 106 describes the significant fields shown in the displays.

Table 106 show mpls l2transport vc detail Field Descriptions

Field	Description
Local interface	Interface on the local router that has been enabled to send and receive Layer 2 packets. The interface varies, depending on the transport type. The output also shows the status of the interface.
line protocol	Status of the line protocol on the edge-facing interface.
Destination address	IP address of the remote router specified for this VC. You specify the destination IP address as part of the **mpls l2transport route** command.
VC ID	Virtual circuit identifier assigned to the interface on the router.
VC status	Status of the VC, which is one of the following: • Admin down—The VC has been disabled by a user. • Down—The VC is not ready to carry traffic between the two VC endpoints. • up—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed. – The disposition interface is programmed if the VC has been configured and the client interface is up. – The imposition interface is programmed if the disposition interface is programmed and a remote VC label and an IGP label exist. The IGP label can be an implicit null in a back-to-back configuration. (An IGP label means there is an LSP to the peer.)
Output interface	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
imposed label stack	Summary of the MPLS label stack used to direct the VC to the PE router.
Preferred path	Path that was assigned to the VC and the status of that path. The path can be a Multiprotocol Label Switching (MPLS) traffic engineering tunnel or an IP address or hostname of a peer PE router.
Default path	Status of the default path, which can be disabled or active. By default, if the preferred path fails, the router uses the default path. However, you can disable the router from using the default path when the preferred path fails by specifying the **disable-fallback** keyword with the **preferred-path** command.

Table 106 show mpls l2transport vc detail Field Descriptions (continued)

Field	Description
Tunnel label	An IGP label used to route the packet over the MPLS backbone to the destination router with the egress interface. The first part of the output displays the type of label. The second part of the output displays the route information. The tunnel label information can display any of the following states: • imp-null: Implicit null means that the provider (P) router is absent and the tunnel label will not be used. Alternatively, imp-null can signify traffic engineering tunnels between the PE routers. • no adjacency: The adjacency for the next hop is missing. • no route: The label is not in the routing table. • not ready, Cisco Express Forwarding disabled: Cisco Express Forwarding is disabled. • not ready, LFIB entry present: The tunnel label exists in the Label Forwarding Information Base (LFIB), but the VC is down. • not ready, LFIB disabled: The MPLS switching subsystem is disabled. • not ready, no route: An IP route for the peer does not exist in the routing table. • not ready, not a host table: The route in the routing table for the remote peer router is not a host route. • unassigned: The label has not been assigned.
Create time	The time (in hours, minutes, and seconds) when the VC was provisioned.
last status change time	Last time (in hours, minutes, and seconds) the VC state changed.
Signaling protocol	Type of protocol used to send the MPLS labels on dynamically configured connections. The output also shows the status of the peer router. For AToM statically configured pseudowires, the field indicates Manual, because there is no exchange of labels using a directed control protocol such as LDP.
MPLS VC labels	Local VC label is a disposition label, which determines the egress interface of an arriving packet from the MPLS backbone. The remote VC label is a disposition VC label of the remote peer router.
Group ID	Local group ID is used to group VCs locally. The remote group ID is used by the peer to group several VCs.
MTU	Maximum transmission unit specified for the local and remote interfaces.
Remote interface description	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
Sequencing	Indicates whether sequencing of out-of-order packets is enabled or disabled.
SSO Descriptor	Identifies the VC for which the information was checkpointed.
local label	The value of the local label that was checkpointed (that is, sent on the active Route Processor [RP], and received on the standby RP).

Table 106 show mpls l2transport vc detail Field Descriptions (continued)

Field	Description
SSM segment/switch IDs	The IDs used to refer to the control plane and data plane for this VC. This data is not for customer use but for Cisco personnel for troubleshooting purposes. When the Source Specific Multicast (SSM) IDs are followed by the word "used," the checkpointed data has been successfully sent and not released.
PWID	The pseudowire ID used in the data plane to correlate the switching context for the segment mentioned with the MPLS switching context. This data is not for customer use but for Cisco personnel for troubleshooting purposes.
packet totals	Number of packets sent and received. Received packets are those AToM packets received from the MPLS core. Sent packets are those AToM packets sent to the MPLS core. This does not include dropped packets. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the router.
byte totals	Number of bytes sent and received from the core-facing interface, including the payload, control word if present, and AToM VC label. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the router.
packet drops	Number of dropped packets. **Note** If the VC statistics fields include the word "transit," the output shows the number of packets and bytes being sent from the router.

The following example shows the command output of the **show mpls l2transport vc detail** command when the VPLS Autodiscovery feature has configured on the VPLS pseudowires. The output that is specific to VPLS Autodiscovery is show in bold.

```
Router# show mpls l2transport vc detail

Local interface: VFI my_test VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.3.3.1, VC ID: 123456, VC status: up
    Next hop PE address: 10.55.55.2
    Output interface: Et3/0, imposed label stack {17 19}
    Preferred path: not configured
    Default path:
    Next hop: 10.1.0.2
  Create time: 2d05h, last status change time: 2d05h

Signaling protocol: LDP, peer 10.55.55.2:0 up
    MPLS VC labels: local 21, remote 19
    AGI: type 1, len 8,  0000 3333 4F4E 44C4
    Local AII:  type 1, len 4, 0909 0909 (10.9.9.9)
    Remote AII: type 1, len 4, 0303 0301 (10.3.3.3)
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 22611, send 22611
    byte totals:   receive 2346570, send 2853581
    packet drops:  receive 0, send 0
```

Table 107 describes the fields shown in the display.

Table 107 show mpls l2transport vc detail Field Descriptions for VPLS Autodiscovery

Field	Description
Next hop PE address	The IP address of the next hop router.
AGI	The attachment group identifier (AGI).
Local AII	The attachment individual identifier (AII). The local IP address used for signaling.
Remote AII	The remote IP address used for signaling. This address is the provisioned IP address, which might not be the same as the LDP peer IP address.

The following example shows sample output from the **show mpls l2 transport vc** command when the CEM interface is specified.

```
Router# show mpls l2transport vc interface CEM 3/1/1

Local intf  Local circuit  Dest address  VC ID  Status
----------  -------------  ------------  -----  ------
CE3/1/1     CESOPSN Basic 10.30.30.3    300    DOWN
```

Table 105 to Table 109 describes the fields shown in the display.

The following example displays (in bold) the number of MAC address withdrawal messages sent and received as part of the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature:

```
Router# show mpls l2transport vc detail

Local interface: VFI TEST VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.1.1.1, VC ID: 1000, VC status: up
    Output interface: Se2/0, imposed label stack {17}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:04:34, last status change time: 00:04:15
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.1
    MPLS VC labels: local 16, remote 17
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent 5, received 3
  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
```

Table 105 to Table 109 describes the fields shown in the display.

The following example displays (in bold) the status messages for the MPLS Pseudowire Status Signaling feature when it is enabled on both PE routers:

```
Router# show mpls l2transport vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 10.1.1.1, VC ID: 456, VC status: up
    Output interface: Et2/0, imposed label stack {10005 10240}
    Preferred path: not configured
```

```
  Default path: active
  Next hop: 10.0.0.1
Create time: 00:39:30, last status change time: 00:26:48
Signaling protocol: LDP, peer 10.1.1.1:0 up
  Targeted Hello: 10.1.1.2(LDP Id) -> 10.1.1.1
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: PW DOWN(rx,tx faults)
MPLS VC labels: local 2000, remote 10240
Group ID: local 6, remote 0
MTU: local 1500, remote 1500
Remote interface description:
  Sequencing: receive disabled, send disabled
VC statistics:
  packet totals: receive 243651, send 243705
  byte totals:   receive 27768366, send 34109320
  packet drops:  receive 0, send 0
```

Table 108 describes the fields shown in the display.

Table 108 show mpls l2transport vc detail Field Descriptions for the MPLS Pseudowire Signaling Status Feature

Field	Description
Status TLV support (local/remote)	For the local router, the output indicates whether the MPLS Pseudowire Signaling Status feature is enabled or disabled. For the remote router, the output indicates whether the MPLS Pseudowire Signaling Status feature is supported.
Label/status state machine	The first value in the output indicates whether label advertisement has been established or not. The second value (LruRru) indicates the status of the local and remote routers. The following list translates the status codes: L—local router R—remote router r or n—ready (r) or not ready (n) u or d—up (u) or down (d) status These values are also displayed in the output: D—Dataplane S—Local shutdown
Last local dataplane status rcvd	The last status message received about the dataplane on the local router.
Last local SSS circuit status rcvd	The last status message received about the subscriber service switch (SSS) on the local router.
Last local SSS circuit status sent	The last status message sent about the subscriber service switch on the local router.

Table 108 show mpls l2transport vc detail Field Descriptions for the MPLS Pseudowire Signaling Status Feature

Field	Description
Last local LDP TLV status sent	The last status message sent about the Type, Length, Value (TLV) on the local router.
Last remote LDP TLV status rcvd	The last status message received about the TLV on the local router.

The following example shows sample output from the **show mpls l2 transport vc** command to display the status of multisegment pseudowires.

```
PE1# show mpls l2transport vc detail

Local interface: Se3/0 up, line protocol up, HDLC up
  Destination address: 12.1.1.1, VC ID: 100, VC status: down
    Output interface: Se2/0, imposed label stack {23}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:03:02, last status change time: 00:01:41
  Signaling protocol: LDP, peer 12.1.1.1:0 up
    Targeted Hello: 11.1.1.1(LDP Id) -> 12.1.1.1, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRrd
      Last local dataplane   status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: DOWN(PW-tx-fault)
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: DOWN(PW-tx-fault)
       PW Switching Point:
       Fault type  Vcid   local IP addr   remote IP addr   Description
       PW-tx-fault  101        13.1.1.1         12.1.1.1   S-PE2
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 19, remote 23
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 16, send 27
    byte totals:   receive 2506, send 3098
    packet drops:  receive 0, seq error 0, send 0
```

Table 109 describes the fields shown in the display.

Table 109 show mpls l2transport vc detail Field Descriptions for the MPLS Multisegment Pseudowire Feature

Field	Description
Fault type	Type of fault encountered on the switching point.
Vcid	The ID of the VC where the fault occurred.
local IP addr	The local IP address of the pseudowire.
remote IP addr	The remote IP address of the pseudowire.
Description	The descriptions assigned to the segment of the pseudowire.

The following example shows sample output from the **show mpls l2 transport vc** command to display the status of the control word when it is not configured; that is, it defaults to autosense.

```
Router# show mpls l2transport vc 123400 detail

Local interface: Et0/0 up, line protocol up, Ethernet up
  Destination address: 10.1.1.2, VC ID: 123400, VC status: down
    Output interface: if-?(0), imposed label stack {}
    Preferred path: not configured
    Default path: no route
    No adjacency
  Create time: 01:03:48, last status change time: 01:03:48
  Signaling protocol: LDP, peer 10.1.1.3:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.2
    Status TLV support (local/remote)   : enabled/unknown (no remote binding)
      Label/status state machine        : local ready, LruRnd
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: not sent
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: unknown (no remote binding)
    MPLS VC labels: local 1002, remote unassigned
    Group ID: local 0, remote unknown
    MTU: local 1500, remote unknown
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: on (configured: autosense)
```

If the control word is negotiated by the peer and is different from the configured value, the configured value is shown in parentheses.

- If the control word is configured to be disabled, the displayed value is:

  Control Word: off (configured: disabled)

- If the control word is configured to be enabled but negotiated by the peer to be off, the displayed value is:

  Control Word: off (configured: enabled)

- If the control word is not configured, the displayed value is:

  Control Word: on (configured: autosense)

Related Commands

Command	Description
show mpls l2transport summary	Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a router.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show mpls label range

To display the range of local labels available for use on packet interfaces, use the **show mpls label range** command in privileged EXEC mode.

show mpls label range

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(9)ST	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The “Usage Guidelines” and the sample command output changed.

Usage Guidelines

You can use the **mpls label range** command to configure a range for local labels that is different from the default range. The **show mpls label range** command displays both the label range currently in use and the label range that will be in use following the next router reload.

Examples

In the following example, the use of the **show mpls label range** command is shown before and after the **mpls label range** command is used to configure a label range that does not overlap the starting label range:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 16/100000

Router# configure terminal

Router(config)# mpls label range 200 120000
Router(config)# exit

Router# show mpls label range

Downstream label pool: Min/Max label: 200/120000
```

Related Commands

Command	Description
mpls label range	Configures a range of values for use as local labels.

show mpls ldp backoff

To display information about the configured session setup backoff parameters and any potential Label Distribution Protocol (LDP) peers with which session setup attempts are being throttled, use the **show mpls ldp backoff** command in user EXEC or privileged EXEC mode.

show mpls ldp backoff [**vrf** *vrf-name* | **all**]

Syntax Description

vrf *vrf-name*	(Optional) Displays backoff information for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
all	(Optional) Displays LDP discovery information for all VPNs.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(30)S	The **vrf** *vrf-name* keyword-argument pair and the **all** keyword were added.
12.4(3)	The **vrf** *vrf-name* keyword-argument pair and the **all** keyword were added.
12.4(4)T	The **vrf** *vrf-name* keyword-argument pair and the **all** keyword were added.
12.0(32)S	The **vrf** *vrf-name* keyword-argument pair and the **all** keyword were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show mpls ldp backoff** command:

```
Router# show mpls ldp backoff

LDP initial/maximum backoff: 30/240 sec
Backoff table: 2 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.144.0.44:0        60             30
10.155.0.55:0        120            90
```

Table 110 describes the significant fields shown in the display.

Table 110 show mpls ldp backoff Field Descriptions

Field	Description
LDP initial/maximum backoff	Indicates the configured backoff parameters (initial and maximum) in seconds.
Backoff table	Contains a list of discovered LDP neighbors for which session setup is being delayed because of previous failures to establish a session due to incompatible configuration. The backoff table incorporates the following information: • LDP Id—Identifies the LDP neighbors. • Backoff(sec)—Shows the amount of time that session setup is being delayed. • Waiting(sec)—Shows the approximate amount of time that session setup has been delayed.

The following is sample output from the **show mpls ldp backoff vrf** *vrf-name* command that shows one entry in the Backoff table for VRF vrf1:

```
Router# show mpls ldp backoff vrf vrf1

LDP initial/maximum backoff: 15/120 sec
VRF vrf1 Backoff table: 1 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.12.0.2:0         120            30
```

The following is sample output from a form of the **show mpls ldp backoff** command using the **all** keyword:

```
Router# show mpls ldp backoff all

LDP initial/maximum backoff: 15/120 sec
Backoff table: 2 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.155.0.55:0       120            30
10.144.0.44:0       60             60

VRF vrf1 Backoff table: 1 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.12.0.2:0         120            45

VRF vrf2 Backoff table: 1 entries
LDP Id              Backoff(sec)   Waiting(sec)
10.13.0.1:0         120            30
```

See Table 110 for a description of the significant fields shown in the displays.

Related Commands

Command	Description
mpls ldp backoff	Configures session setup delay parameters for the LDP backoff mechanism.

show mpls ldp bindings

To display the contents of the Label Information Base (LIB), use the **show mpls ldp bindings** command in user EXEC or privileged EXEC mode.

show mpls ldp bindings [**vrf** *vrf-name* | **all**] [*network* {*mask* | *length*} [**longer-prefixes**]] [**local-label** *label* [- *label*]] [**remote-label** *label* [- *label*]] [**neighbor** *address* | **local**] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the label bindings for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
all	(Optional) Displays LIB information for all VPNs.
network	(Optional) Destination network number.
mask	Network mask, written as A.B.C.D.
length	Mask length (1 to 32 characters).
longer-prefixes	(Optional) Selects any prefix that matches the value in the *mask* argument with a *length* from 1 to 32 characters.
local-label *label - label*	(Optional) Display entries matching local label values. Use the *label - label* arguments and keyword to indicate the label range. The hyphen (-) keyword is required for a label range.
remote-label *label - label*	(Optional) Displays entries matching the label values assigned by a neighbor router. Use the *label - label* arguments and keyword to indicate the label range. The hyphen (-) keyword is required for a label range.
neighbor *address*	(Optional) Displays the label bindings assigned by the selected neighbor.
local	(Optional) Displays the local label bindings.
detail	(Optional) Displays the checkpoint status of the local label bindings.

Defaults

If no optional keywords or arguments are entered, the command displays the LIB for the default routing domain only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was modified to support Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified to include MPLS Virtual Private Network (VPN) support for Label Distribution Protocol (LDP).
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Release	Modification
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **detail** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The output of the command was updated to display information about LDP local label allocation filtering.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **show mpls ldp bindings** command displays label bindings learned by the LDP or Tag Distribution Protocol (TDP).

Note TDP is not supported for LDP features in Cisco IOS 12.0(30)S and later releases, 12.2(28)SB and later 12.2S releases, and 12.3(14)T and later releases.

A request can specify that the entire database be displayed, or that the display be limited to a subset of entries according to the following:

- Prefix
- Input or output label values or ranges
- Neighbor advertising the label

Note The **show mpls ip binding** command includes the output generated by the **show mpls ldp bindings** command. On the Cisco 7000 series router, this command displays information about label bindings for LC-ATM interfaces.

Examples

The following is sample output from the **show mpls ldp bindings** command. This form of the command displays the contents of the LIB for the default routing domain.

```
Router# show mpls ldp bindings

  10.0.0.0/8, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.10.0.55:0, label: 17
        remote binding: lsr: 10.66.0.66:0, label: 18
        remote binding: lsr: 10.0.0.44:0, label: imp-null
  172.16.0.0/8, rev 17
        local binding:  label: 19
```

```
        remote binding: lsr: 10.0.0.55:0, label: imp-null
        remote binding: lsr: 10.66.0.66:0, label: 16
        remote binding: lsr: 10.0.0.44:0, label: imp-null
  192.168.0.66/32, rev 19
        local binding:  label: 20
        remote binding: lsr: 10.0.0.55:0, label: 19
        remote binding: lsr: 10.66.0.66:0, label: imp-null
        remote binding: lsr: 10.0.0.44:0, label: 18
       .
       .
       .
```

The following is sample output from the **show mpls ldp bindings** *network length* **longer-prefixes neighbor** *address* variant of the command; it displays labels learned from label switch router (LSR) 10.144.0.44 for network 10.166.0.0 and any of its subnets. The use of the **neighbor** keyword suppresses the output of local labels and labels learned from other neighbors.

```
Router# show mpls ldp bindings 10.166.0.0 8 longer-prefixes neighbor 10.144.0.44

  10.166.44.0/16, rev 31
        remote binding: lsr: 10.144.0.44:0, label: 25
  10.166.45.0/16, rev 33
        remote binding: lsr: 10.144.0.44:0, label: 26
  10.166.245.0/16, rev 71
        remote binding: lsr: 10.144.0.44:0, label: 45
  10.166.246.0/16, rev 73
        remote binding: lsr: 10.144.0.44:0, label: 46
.
.
.
```

The following is sample output from the **show mpls ldp bindings vrf vpn1** command, which displays the label bindings for the specified VPN routing and forwarding instance named vpn1:

```
Router# show mpls ldp bindings vrf vpn1

  10.3.3.0/16, rev 164
        local binding: label:117
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.13.13.13/32, rev 1650
        local binding: label:1372
        remote binding:lsr:10.14.14.14:0, label:268
  10.14.14.14/32, rev 165
        local binding: label:118
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.15.15.15/32, rev 1683
        local binding: label:1370
        remote binding:lsr:10.14.14.14:0, label:266
  10.16.16.16/32, rev 775
        local binding: label:8370
        remote binding:lsr:10.14.14.14:0, label:319
  10.18.18.18/32, rev 1655
        local binding: label:21817
        remote binding:lsr:10.14.14.14:0, label:571
  10.30.2.0/16, rev 1653
        local binding: label:6943
        remote binding:lsr:10.14.14.14:0, label:267
  10.30.3.0/16, rev 413
        local binding: label:2383
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.30.4.0/16, rev 166
        local binding: label:77
        remote binding:lsr:10.14.14.14:0, label:imp-null
```

```
  10.30.5.0/16, rev 1429
        local binding: label:20715
        remote binding:lsr:10.14.14.14:0, label:504
  10.30.7.0/16, rev 4
        local binding: label:17
        remote binding:lsr:10.14.14.14:0, label:imp-null
  10.30.10.0/16, rev 422
        local binding: label:5016
        remote binding:lsr:10.14.14.14:0, label:269
.
.
.
```

The following is sample output from the **show mpls ldp bindings all** command, which displays the label bindings for all VRFs:

```
Router# show mpls ldp bindings all

  lib entry: 10.0.0.0/24, rev 4
        local binding:  label: imp-null
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.11.0.0/24, rev 15
        local binding:  label: imp-null
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.101.0.1/32, rev 18
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.131.0.1/32, rev 17
        local binding:  label: 20
        remote binding: lsr: 10.131.0.1:0, label: imp-null
  lib entry: 10.134.0.1/32, rev 6
        local binding:  label: imp-null
        remote binding: lsr: 10.131.0.1:0, label: 16
VRF vrf1:
  lib entry: 10.0.0.0/24, rev 6
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.11.0.0/24, rev 7
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.12.0.0/24, rev 8
        local binding:  label: 17
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.132.0.1/32, rev 4
        remote binding: lsr: 10.132.0.1:0, label: imp-null
  lib entry: 10.134.0.2/32, rev 9
        local binding:  label: 18
        remote binding: lsr: 10.132.0.1:0, label: 16
  lib entry: 10.134.0.4/32, rev 10
        local binding:  label: 19
        remote binding: lsr: 10.132.0.1:0, label: 17
  lib entry: 10.138.0.1/32, rev 5
        remote binding: lsr: 10.132.0.1:0, label: imp-null
```

The following is sample output from the **show mpls ldp bindings detail** command:

```
Router# show mpls ldp bindings detail

lib entry: 10.3.3.0/16, rev 2,
        local binding:  label: imp-null
          Advertised to:
          10.20.20.20:0          10.25.25.25:0
        remote binding: lsr: 10.20.20.20:0, label: imp-null  stale
        remote binding: lsr: 10.25.25.25:0, label: imp-null  stale
  lib entry: 10.13.1.0/24, rev 4,
        local binding:  label: imp-null
          Advertised to:
```

```
        10.20.20.20:0          10.25.25.25:0
      remote binding: lsr: 10.20.20.20:0, label: imp-null  stale
      remote binding: lsr: 10.25.25.25:0, label: 16  stale
  lib entry: 10.13.2.0/24, rev 6,
      local binding:  label: imp-null
        Advertised to:
        10.20.20.20:0          10.25.25.25:0
      remote binding: lsr: 10.20.20.20:0, label: 16  stale
      remote binding: lsr: 10.25.25.25:0, label: imp-null  stale
  lib entry: 10.6.1.0/24, rev 22,
      local binding:  label: 21
        Advertised to:
        10.20.20.20:0          10.25.25.25:0
      remote binding: lsr: 10.20.20.20:0, label: 19  stale
      remote binding: lsr: 10.25.25.25:0, label: imp-null  stale
```

The following is sample output from the **show mpls ldp bindings detail** command when LDP local label allocation filtering is configured:

```
Router# show mpls ldp bindings detail

Advertisement spec:
        Prefix acl = bar
Local label filtering spec: host routes.


  lib entry: 10.1.1.1/32, rev 9
  lib entry: 10.10.7.0/24, rev 10
  lib entry: 10.10.8.0/24, rev 11
  lib entry: 10.10.9.0/24, rev 12
  lib entry: 10.41.41.41/32, rev 17
  lib entry: 10.50.50.50/32, rev 15
  lib entry: 10.60.60.60/32, rev 18
  lib entry: 10.70.70.70/32, rev 16
  lib entry: 10.80.80.80/32, rev 14
```

Table 111 describes the significant fields shown in the displays.

Table 111 show mpls ldp bindings Field Descriptions

Field	Description
10.3.3.0/16 10.1.1.1/32	IP prefix and mask for a particular destination (network/mask).
rev 9	Revision number that is used internally to manage label distribution for this destination.
Advertised to	The LSRs that received the label binding.
local binding	Labels assigned by the local LSR.
remote binding	List of outgoing labels for this destination learned from other LSRs. Each item in this list identifies the LSR from which the outgoing label was learned and the label itself. The LSR is identified by its LDP identifier.
stale	After an LDP session is lost and the routers begin a graceful restart, the remote label bindings are marked stale.
Local label filtering spec: host routes.	LDP allocates local labels for host routes.

Related Commandst

Command	Description
show mpls ip binding	Displays specified information about label bindings learned by the MPLS LDP.
show mpls ldp neighbor	Displays the status of LDP sessions.

show mpls ldp checkpoint

To display information about the Label Distribution Protocol (LDP) checkpoint system on the active route processor, use the **show mpls ldp checkpoint** command in user EXEC or privileged EXEC mode.

show mpls ldp checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command shows the following LDP checkpointing information:

- The status of the checkpointing system
- The status of the resend timer
- The number of Label Information Base (LIB) entries in a checkpointed state

This command displays checkpoint status information only for the active route processor.

Examples

The following example shows the LDP checkpoint settings and configuration:

```
Router# show mpls ldp checkpoint

Checkpoint status: dynamic-sync
Checkpoint resend timer: not running
5 local bindings in add-skipped
9 local bindings in added
1 of 15+ local bindings in none
```

Table 112 describes the significant fields shown in the display.

Table 112 show mpls ldp checkpoint Field Descriptions

Field	Description
Checkpoint status	The status of the checkpointing system. If the status shows dynamic-sync or another enabled state, then the checkpointing system is enabled. If the status shows disabled, then the checkpointing system is disabled.
Checkpoint resend timer	The status of the resend timer.
local bindings in add-skipped	The number of local bindings that were not checkpointed, because they do not need to be checkpointed. For example, local label bindings using null labels are not checkpointed.
local bindings in added	The number of local bindings that were copied to the standby route processor.
local bindings in none	The number of local bindings that reside on the active route processor and need to be copied to the backup route processor.

Related Commands

Command	Description
show mpls ldp graceful-restart	Displays a summary of the LDP Graceful Restart status.

show mpls ldp discovery

To display the status of the Label Distribution Protocol (LDP) discovery process, use the **show mpls ldp discovery** command in user EXEC or privileged EXEC mode.

show mpls ldp discovery [**vrf** *vrf-name* | **all**] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the neighbor discovery information for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
all	(Optional) Displays LDP discovery information for all VPNs, including those in the default routing domain.
detail	(Optional) Displays detailed information about all LDP discovery sources on a label switch router (LSR).

Defaults

This command displays neighbor discovery information for the default routing domain if an optional **vrf** keyword is not specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST. The command was modified to comply with Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified for MPLS VPN support for LDP. The **vrf** and **all** keywords were added.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was modified for MPLS VPN support for LDP. The **vrf** and **all** keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(14)T	The **detail** keyword was added to the command to display information related to the LDP Autoconfiguration feature.
12.2(28)SB	The **detail** keyword was updated to display information related to LDP Message Digest 5 (MD5) password configuration.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S and LDP MD5 password rollover information displays in the command output when the **detail** argument is used with the **show mpls ldp discovery** command.

Usage Guidelines

This command displays neighbor discovery information for LDP or Tag Distribution Protocol (TDP). It generates a list of interfaces over which the LDP discovery process is running.

Examples

The following is sample output from the **show mpls ldp discovery** command:

```
Router# show mpls ldp discovery

Local LDP Identifier:
    10.1.1.1:0
Discovery Sources:
    Interfaces:
        Ethernet1/1/3 (ldp): xmit/recv
            LDP Id: 172.23.0.77:0
            LDP Id: 10.144.0.44:0
            LDP Id: 10.155.0.55:0
        ATM3/0.1 (ldp): xmit/recv
            LDP Id: 10.203.0.7:2
        ATM0/0.2 (tdp): xmit/recv
            TDP Id: 10.119.0.1:1
Targeted Hellos:
        10.8.1.1 -> 10.133.0.33 (ldp): active, xmit/recv
            LDP Id: 10.133.0.33:0
        10.8.1.1 -> 192.168.7.16 (tdp): passive, xmit/recv
            TDP Id: 10.133.0.33:0
Router#
```

The following is sample output from the **show mpls ldp discovery all** command, which shows the interfaces engaged in LDP discovery activity for all the VPN routing and forwarding instances, including those in the default routing domain. In this example, note that the same neighbor LDP ID (10.14.14.14) appears in all the listed VRF interfaces, highlighting the fact that the same IP address can coexist in different VPN routing and forwarding instances.

```
Router# show mpls ldp discovery all

Local LDP Identifier:
    10.12.12.12:0
    Discovery Sources:
    Interfaces:
        ATM1/1/0.1 (tdp):xmit/recv
            TDP Id:10.11.11.11:0
VRF vpn1:Local LDP Identifier:
    172.30.7.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.1 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn2:Local LDP Identifier:
    172.30.13.2:0
```

```
    Discovery Sources:
    Interfaces:
        ATM3/0/0.2 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn3:Local LDP Identifier:
    172.30.15.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.3 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn4:Local LDP Identifier:
    172.30.17.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.4 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn5:Local LDP Identifier:
    172.30.19.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.5 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn6:Local LDP Identifier:
    172.30.21.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.6 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn7:Local LDP Identifier:
    172.23.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.7 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn8:Local LDP Identifier:
    172.30.25.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.8 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn9:Local LDP Identifier:
    172.30.27.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.9 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn10:Local LDP Identifier:
    172.30.29.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.10 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn11:Local LDP Identifier:
    172.30.31.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.11 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn12:Local LDP Identifier:
    172.30.33.2:0
    Discovery Sources:
```

```
    Interfaces:
        ATM3/0/0.12 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn13:Local LDP Identifier:

Router#
```

Table 113 describes the significant fields shown in the display.

Table 113 show mpls ldp discovery Field Descriptions

Field	Description
Local LDP Identifier	The LDP identifier for the local router. An LDP identifier is 6-bytes displayed in the form “IP address:number.” By convention, the first four bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.
Interfaces	Lists the interfaces that are engaging in LDP discovery activity: • The xmit field—Indicates that the interface is sending LDP discovery hello packets. • The recv field—Indicates that the interface is receiving LDP discovery hello packets. • The (LDP) or (TDP) field—Indicates the Label Distribution Protocol or Tag Distribution Protocol configured for the interface. The LDP (or TDP) identifiers indicate the LDP (or TDP) neighbors discovered on the interface.
Targeted Hellos	Lists the platforms to which targeted hello messages are being sent: • The xmit, recv, (ldp), and (tdp) fields are as described for the Interfaces field. • The active field indicates that this LSR has initiated targeted hello messages. • The passive field indicates that the neighbor LSR has initiated targeted hello messages and that this LSR is configured to respond to the targeted hello messages from the neighbor. **Note** The entry for a given target platform may indicate both active and passive.

The following is sample output from the **show mpls ldp discovery detail** command showing that LDP was enabled by the **mpls ip** command and the **mpls ldp autoconfig** command:

```
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: 172.140.0.1; Transport IP addr: 10.10.10.10
  Hold time: 15 sec; Proposed local/peer: 15/15 sec
```

Table 114 describes the significant fields shown in the display.

Table 114 show mpls ldp discovery detail Field Descriptions

Field	Description
Local LDP Identifier	The LDP identifier for the local router. An LDP identifier is a 6-byte construct displayed in the form “IP address:number.” By convention, the first four bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.
Interfaces	Lists the interfaces that are engaging in LDP discovery activity: • The xmit field—Indicates that the interface is sending LDP discovery hello packets. • The recv field—Indicates that the interface is receiving LDP discovery hello packets. • The (LDP) or (TDP) field—Indicates the Label Distribution Protocol or Tag Distribution Protocol configured for the interface. The LDP (or TDP) identifiers indicate the LDP (or TDP) neighbors discovered on the interface.
Interface config, IGP config;	Describes how LDP is enabled: • Interface config—Enabled by the **mpls ip** command. • IGP config—Enabled by the **mpls ldp autoconfig** command. • Interface config, IGP config;—Enabled by the **mpls ip** command and the **mpls ldp autoconfig** command.
Hello interval	Period of time (in milliseconds) between the sending of consecutive hello messages.
Transport IP addr	Specifies that the interface address should be advertised as the transport address in the LDP discovery hello messages.
LDP Id	LDP ID of the peer router.
Src IP addr	Source IP address of the local router.
Transport IP addr	Specifies that the named IP address should be advertised as the transport address in the LDP discovery hello messages sent on an interface.
Hold time	Period of time (in seconds) a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
Proposed local/peer	Hold times (in seconds) proposed for LDP hello timer by the local router and the peer router. LDP uses the lower of these two values as the hold time.

The following is sample output from the **show mpls ldp discovery detail** command, which displays information related to LDP MD5 passwords. Information related to MD5 passwords is pointed out in bold text in the output.

```
Router# show mpls ldp discovery detail

 Local LDP Identifier:
    10.10.10.10:0
    Discovery Sources:
    Interfaces:
        Ethernet1/0 (ldp): xmit/recv
            Hello interval: 5000 ms; Transport IP addr: 10.10.10.10
            LDP Id: 10.4.4.4:0
              Src IP addr: 10.0.20.4; Transport IP addr: 10.4.4.4
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
              Password: not required, none, stale       <-- LDP MD5 password information
    Targeted Hellos:
        10.10.10.10 -> 10.3.3.3 (ldp): passive, xmit/recv
            Hello interval: 10000 ms; Transport IP addr: 10.10.10.10
            LDP Id: 10.3.3.3:0
              Src IP addr: 10.3.3.3; Transport IP addr: 10.3.3.3
              Hold time: 90 sec; Proposed local/peer: 90/90 sec
              Password: required, neighbor, in use     <-- LDP MD5 password information
```

Password information displayed by this command includes:

- Password requirement for the neighbor (required or not required).
- Password source in the current configuration. The source is described by one of the following:
  - neighbor—The password for the neighbor is retrieved from the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password* command. The *ip-address* argument is the router ID of the neighbor.
  - num—The password for the neighbor is retrieved from **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password* command. The *number* argument is a number from 1 to 32767. The *acl* argument is the name or number of an IP standard access list that permits the neighbor router ID.
  - fallback—The password for the neighbor is retrieved from **mpls ldp** [**vrf** *vrf-name*] **password fallback** *password* command.
  - none—No password is configured for this neighbor.
- Password used by LDP sessions established with the neighbor is from current or previous configuration (in use or stale).

Related Commands

Command	Description
mpls label protocol (global configuration)	Specifies the LDP or TDP to be used on a platform.
mpls label protocol (interface configuration)	Specifies the LDP or TDP to be used on a given interface.
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.

Command	Description
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS label switch router (LSR).
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.

show mpls ldp graceful-restart

To display a summary of the Label Distribution Protocol (LDP) Graceful Restart status, use the **show mpls ldp graceful-restart** command in user EXEC or privileged EXEC mode.

show mpls ldp graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command shows the following information about LDP sessions:

- Configured parameters.
- The state of the LDP sessions (for which Graceful Restart was negotiated during initialization).
- The list of LDP sessions for which graceful recovery is pending. However, the router has retained the state information from those neighbors.

Examples

The following example shows a summary of the LDP Graceful Restart settings and configuration:

```
Router# show mpls ldp graceful-restart

LDP Graceful Restart is enabled
Neighbor Liveness Timer: 5 seconds
Max Recovery Time: 200 seconds
Down Neighbor Database (0 records):
Graceful Restart-enabled Sessions:
VRF default:
    Peer LDP Ident: 10.18.18.18:0, State: estab
    Peer LDP Ident: 10.17.17.17:0, State: estab
```

Table 115 describes the significant fields shown in the display.

Table 115 show mpls ldp graceful-restart Field Descriptions

Field	Description
Neighbor Liveness Timer	The number of seconds the neighbor liveness timer is set for.
Max Recovery Time	The number of seconds the maximum recovery timer is set for.
Down Neighbor Database	Information about the down (failed or restarting) LDP neighbor.
Graceful Restart-enabled Sessions	Information about the LDP sessions that are enabled for Graceful Restart.
Peer LDP Ident	The LDP ID of the provider edge (PE) neighbor.
State	The state of the session with the neighbor.

Related Commands

Command	Description
show mpls ldp neighbor	Displays the status of LDP sessions.

show mpls ldp igp sync

To display the status of the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization process, use the **show mpls ldp igp sync** command in user EXEC or privileged EXEC mode.

show mpls ldp igp sync [**all** | **interface** *type number* | **vrf** *vpn-name*]

Syntax Description

all	(Optional) Display IGP SYNC information in all VPN routing and forwarding (VRF) instances.
interface *type number*	(Optional) Displays the MPLS LDP-IGP synchronization information for the specified interface.
vrf *vpn-name*	(Optional) Displays the MPLS LDP-IGP synchronization information for the specified VRF instance (*vpn-name*).

Command Default

If an optional argument is not specified, this command displays LDP synchronization for all interfaces enabled for MPLS LDP-IGP synchronization.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.0(32)S	This command was integrated into Cisco IOS Release 12.0(32)S. The output of this command was changed to display the configured delay time and the time remaining on the delay timer.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. The **all** keyword was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)M	This command was integrated into Cisoc IOS Release 15.0(1)M.

Examples

The following is sample output from the **show mpls ldp igp sync** command:

```
Router# show mpls ldp igp sync

Ethernet0/0:
 LDP configured;  SYNC enabled.
 SYNC status: sync achieved; peer reachable.
 IGP holddown time: infinite.
 Peer LDP Ident: 10.130.0.1:0
 IGP enabled: OSPF 1
```

Table 116 describes the significant fields shown in the display.

Table 116 show mpls ldp igp sync Field Descriptions

Field	Description
Ethernet0/0	Interface name and type.
LDP configured	Label Distribution Protocol is configured.
SYNC enabled	Synchronization is active.
SYNC status	Synchronization is successful. **Note** Peer reachable is an LDP internal state used only for MPLS LDP synchronization. Do not use it to verify that LDP can reach the peer or to troubleshoot LDP functionality.
IGP holddown time	Interior Gateway Protocol hold-down time. • Infinite—No specific time is set.
Peer LDP Ident	IP address of the peer.
IGP enabled	Interior Gateway Protocol is enabled for the specified Open Shortest Path First (OSPF) protocol.

If LDP-IGP synchronization is not enabled on an interface, the output looks like the following:

```
Router# show mpls ldp igp sync

Ethernet5/1:
 LDP configured; LDP-IGP Synchronization not enabled.
```

The following is sample output from the **show mpls ldp igp sync** command when you configured a time delay for MPLS LDP-IGP synchronization:

```
Router# show mpls ldp igp sync

Ethernet0/0:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: sync achieved; peer reachable.
 Sync delay time: 20 seconds (10 seconds left)
 IGP holddown time: infinite.
 IGP enabled: OSPF 1
```

Related Commands

Command	Description
debug mpls ldp igp sync	Displays events related to MPLS LDP-IGP synchronization.
mpls ldp igp sync	Enables MPLS LDP-IGP synchronization on an interface that belongs to an OSPF process.
mpls ldp igp sync holddown	Specifies how long an IGP should wait for LDP synchronization to be achieved.
mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces for an OSPF process or an IS-IS process.

show mpls ldp neighbor

To display the status of Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor** command in user EXEC or privileged EXEC mode.

show mpls ldp neighbor [**vrf** *vrf-name* | **all**] [*address* | *interface*] [**detail**] [**graceful-restart**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
all	(Optional) Displays LDP neighbor information for all VPNs, including those in the default routing domain.
address	(Optional) Identifies the neighbor with this IP address.
interface	(Optional) Identifies the LDP neighbors accessible over this interface.
detail	(Optional) Displays information in long form, including password information for this neighbor.
graceful-restart	(Optional) Displays per-neighbor graceful restart information.

Defaults

This command displays information about LDP neighbors for the default routing domain if you do not specify the optional **vrf** keyword.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	The command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP and the **vrf** and **all** keywords were added.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(26)S	The **detail** keyword was updated to display information about inbound filtering.
12.2(25)S	The **graceful-restart** keyword was added.
12.3(14)T	The command output was updated so that the **detail** keyword displays information about MPLS LDP Session Protection.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Release	Modification
12.2(28)SB	The **detail** keyword was updated to include Message Digest 5 (MD5) password information and the command was implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show mpls ldp neighbor** command can provide information about all LDP neighbors, or the information can be limited to the following:

- Neighbor with specific IP address
- LDP neighbors known to be accessible over a specific interface

Note This command displays information about LDP and Tag Distribution Protocol (TDP) neighbor sessions.

Examples

The following is sample output from the **show mpls ldp neighbor** command:

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        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         10.0.0.199      10.10.1.1
          10.205.0.9
```

The following is sample output from the **show mpls ldp neighbor** command, in which duplicate addresses are detected. They indicate an error because a given address should be bound to only one peer.

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        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 10.0.0.199 10.10.1.1
          10.205.0.9
        Duplicate Addresses advertised by peer:
          10.10.8.111
```

The following is sample output from the **show mpls ldp neighbor vrf vpn10** command, which displays the LDP neighbor information for the specified VPN routing and forwarding instance named vpn10:

```
Router# show mpls ldp neighbor vrf vpn10

Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.29.0.2:0
        TCP connection:10.14.14.14.646 - 10.29.0.2.11384
        State:Oper; Msgs sent/rcvd:1423/800; Downstream
        Up time:02:38:11
        LDP discovery sources:
          ATM3/0/0.10
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
```

The following is sample output from the **show mpls ldp neighbor detail** command, which displays information about inbound filtering:

```
Router# show mpls ldp neighbor vrf vpn1 detail

 Peer LDP Ident: 10.13.13.13:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.13.13.13.646 - 10.33.0.2.31581
   State: Oper; Msgs sent/rcvd: 11/10; Downstream; Last TIB rev sent 13
   Up time: 00:02:25; UID: 26; Peer Id 0;
   LDP discovery sources:
    Ethernet1/0/2; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.105.1       10.13.13.13     10.33.0..1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl:1
 Peer LDP Ident: 10.14.14.14:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.14.14.14.646 - 10.33.0.2.31601
   State: Oper; Msgs sent/rcvd: 10/9; Downstream; Last TIB rev sent 13
   Up time: 00:01:17; UID: 29; Peer Id 3;
   LDP discovery sources:
    Ethernet1/0/3; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.104.1       10.14.14.14     10.32.0.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl:1
```

The following is sample output from the **show mpls ldp neighbor all** command, which displays the LDP neighbor information for all VPN routing and forwarding instances, including those in the default routing domain. In this example, note that the same neighbor LDP ID (10.14.14.14) appears in all the listed VRF interfaces, highlighting the fact that the same IP address can coexist in different VPN routing and forwarding instances.

```
Router# show mpls ldp neighbor all

Peer TDP Ident:10.11.11.11:0; Local TDP Ident 10.12.12.12:0
        TCP connection:10.11.11.11.711 - 10.12.12.12.11003
        State:Oper; PIEs sent/rcvd:185/187; Downstream
        Up time:02:40:02
        TDP discovery sources:
          ATM1/1/0.1
        Addresses bound to peer TDP Ident:
          10.3.38.3        10.1.0.2        10.11.11.11
VRF vpn1:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.7.0.2:0
        TCP connection:10.14.14.14.646 - 10.7.0.2.11359
        State:Oper; Msgs sent/rcvd:952/801; Downstream
        Up time:02:38:49
        LDP discovery sources:
          ATM3/0/0.1
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn2:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.13.0.2:0
        TCP connection:10.14.14.14.646 - 10.13.0.2.11361
        State:Oper; Msgs sent/rcvd:964/803; Downstream
        Up time:02:38:50
        LDP discovery sources:
          ATM3/0/0.2
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn3:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.15.0.2:0
        TCP connection:10.14.14.14.646 - 10.15.0.2.11364
```

```
        State:Oper; Msgs sent/rcvd:1069/800; Downstream
        Up time:02:38:52
        LDP discovery sources:
          ATM3/0/0.3
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.17.0.1       10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn4:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.17.0.2:0
        TCP connection:10.14.14.14.646 - 10.17.0.2.11366
        State:Oper; Msgs sent/rcvd:1199/802; Downstream
```

The following is sample output from the **show mpls ldp neighbor graceful-restart** command, which shows the Graceful Restart status of the LDP neighbors:

```
Router# show mpls ldp neighbor graceful-restart

Peer LDP Ident: 10.20.20.20:0; Local LDP Ident 10.17.17.17:0
   TCP connection: 10.20.20.20.16510 - 10.17.17.17.646
    State: Oper; Msgs sent/rcvd: 8/18; Downstream
    Up time: 00:04:39
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
Peer LDP Ident: 10.19.19.19:0; Local LDP Ident 10.17.17.17:0
    TCP connection: 10.19.19.19.11007 - 10.17.17.17.646
    State: Oper; Msgs sent/rcvd: 8/38; Downstream
    Up time: 00:04:30
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

The following sample output from the **show mpls ldp neighbor detail** command, which displays information about the MD5 password configuration:

```
Router# show mpls ldp neighbor detail

    Peer LDP Ident: 10.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 167/167; Downstream; Last TIB rev sent 9
        Up time: 02:24:02; UID: 5; Peer Id 3;
        LDP discovery sources:
          Targeted Hello 10.1.1.1 -> 10.3.3.3, passive;
            holdtime: 90000 ms, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          10.3.3.3        10.0.30.3
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 9/9; Downstream; Last TIB rev sent 9
        Up time: 00:05:35; UID: 6; Peer Id 1;
        LDP discovery sources:
          Ethernet1/0; Src IP addr: 10.0.20.4
            holdtime: 15000 ms, hello interval: 5000 ms
```

```
Addresses bound to peer LDP Ident:
  10.0.40.4       10.4.4.4         10.0.20.4
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

Table 117 describes the significant fields shown in the displays.

Table 117 show mpls ldp neighbor Field Descriptions

Field	Description
Peer LDP Ident	LDP (or TDP) identifier of the neighbor (peer) for this session.
Local LDP Ident	LDP (or TDP) identifier for the local label switch router (LSR) for this session.
TCP connection	TCP connection used to support the LDP session, shown in the following format: • peer IP address.peer port • local IP address.local port
Password	Indicates if password protection is being used. Password status is as follows: • Required or not required—Indicates whether password configuration is required. • Neighbor, none, option #, or fallback—Indicates the password source when the password was configured. • In use (current) or stale (previous)—Indicates the current LDP session password usage status.
State	State of the LDP session. Generally, this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.
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 only when the peer requests them.
Downstream	Indicates that the downstream method of label distribution is being used for this LDP session. When the downstream method is used, an LSR advertises all of its locally assigned (incoming) labels to its LDP peer (subject to any configured access list restrictions).
Up time	Length of time (in hours, minutes, seconds) the LDP session has existed.
Graceful Restart enabled	Indicates whether the LDP session has Graceful Restart enabled.
Peer reconnect time	The length of time, in milliseconds (ms), the peer router waits for a router to reconnect.
LDP discovery sources	Sources of LDP discovery activity that led to the establishment of this LDP session.

Table 117 show mpls ldp neighbor Field Descriptions (continued)

Field	Description
Targeted Hello	Lists the platforms to which targeted hello messages are being sent: • The active field indicates that this LSR has initiated targeted hello messages. • The passive field indicates that the neighbor LSR has initiated targeted hello messages and that this LSR is configured to respond to the targeted hello messages from the neighbor.
holdtime	Period of time, in milliseconds (ms), a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
hello interval	Period of time, in milliseconds (ms), between the sending of consecutive hello messages.
Addresses bound to peer LDP Ident	Known interface addresses of the LDP session peer. These are addresses that might appear as "next hop" addresses in the local routing table. They are used to maintain the Label Forwarding Information Base (LFIB).
Duplicate Addresses advertised by peer	IP addresses that are bound to another peer. They indicate an error because a given address should be bound to only one peer.
Peer holdtime	The time, in milliseconds (ms), that the neighbor session is retained without the receipt of an LDP message from the neighbor.
KA Interval	Keepalive Interval. The amount of time, in milliseconds (ms), that a router lets pass without sending an LDP message to its neighbor. If this time elapses and the router has nothing to send, it sends a Keepalive message.
Peer state	State of the peer; estab means established.
LDP inbound filtering accept acl:1	Access list that is permitted for inbound label binding filtering.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.

show mpls ldp neighbor password

To display password information used in established Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor password** command in user EXEC mode or privileged EXEC mode.

show mpls ldp neighbor [**vrf** *vrf-name*] [*ip-address* | *interface*] **password** [**pending** | **current**] [**all**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
ip-address	(Optional) Identifies the neighbor that has this IP address.
interface	(Optional) Identifies the LDP neighbors accessible over this interface.
pending	(Optional) Displays LDP sessions whose password is different from that in the current configuration.
current	(Optional) Displays LDP sessions whose password is the same as that in the current configuration.
all	(Optional) When the **all** keyword is specified alone in this command, the command displays LDP password information for all neighbors in all VPNs, including those in the global routing table.

Defaults

If you do not specify an optional keyword for this command, password information for all established LDP sessions is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to display password information for established LDP sessions. If you do not specify an option, password information for all established LDP sessions is displayed. To display LDP sessions whose password is the same as that in the current configuration, use the **current** keyword with the command. To display LDP sessions whose password is different from that in the current configuration, use the **pending** keyword with the command.

Examples

The following is sample output from the **show mpls ldp neighbor password** command, which displays information for all established LDP sessions:

```
Router# show mpls ldp neighbor password

    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.10.01.10.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57
    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215
```

The following is sample output from the **show mpls ldp neighbor password pending** command, which displays information for LDP sessions whose passwords are different from those in the current configuration:

```
Router# show mpls ldp neighbor password pending

    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57
```

The following is sample output from the **show mpls ldp neighbor password current** command, which displays information for LDP sessions whose passwords are the same as those in the current configuration:

```
Router# show mpls ldp neighbor password current

    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215
```

Table 118 describes the significant fields shown in the displays.

Table 118 show mpls ldp neighbor password Field Descriptions

Field	Description
Peer LDP Ident	LDP identifier of the neighbor (peer) for this session.
Local LDP Ident	LDP identifier for the local label switch router (LSR) for this session.
TCP connection	TCP connection used to support the LDP session, shown in the following format: • peer IP address.peer port • local IP address.local port

Table 118 show mpls ldp neighbor password Field Descriptions (continued)

Field	Description
Password	Indicates the password source and status. • Required or not required indicates whether password configuration is required or not. • Neighbor, none, option #, or fallback indicates the password source when the password was configured. None indicates that no password was configured. • In use (current) or stale (previous) is the usage status of the current LDP session password.
State	State of the LDP session. Generally this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Numbers of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintaining the LDP session.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
mpls ldp password rollover duration	Configures the duration before the new password takes effect on an MPLS LSR.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays the status of LDP sessions.
show mpls ldp neighbor password	Displays password information used in established LDP sessions.

show mpls ldp parameters

To display current Label Distribution Protocol (LDP) parameters, use the **show mpls ldp parameters** command in user EXEC or privileged EXEC mode.

show mpls ldp parameters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST. The command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000-PRE2 router.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show mpls ldp parameters** command:

```
Router# show mpls ldp parameters

Protocol version: 1
Downstream label pool: min label 16; max label 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 180 sec; interval: 5 sec
LDP for targeted sessions; peer acl: 1
LDP initial/maximum backoff: 30/240 sec
Router#
```

Table 119 describes the significant fields shown in the display.

Table 119 show mpls ldp parameters Field Descriptions

Field	Description
Protocol version	Indicates the version of LDP running on the platform.
Downstream label pool	Describes the range of labels available for the platform to assign for label switching purposes. The available labels range from the smallest label value (min label) to the largest label value (max label), with a modest number of labels at the low end of the range (reserved labels) reserved for diagnostic purposes.
Session hold time	Indicates the time (in seconds) that an LDP session is to be maintained with an LDP peer without receiving LDP traffic or an LDP keepalive message from the peer.
keep alive interval	Indicates the interval of time (in seconds) between consecutive transmissions of LDP keepalive messages to an LDP peer.
Discovery hello	Indicates the amount of time (in seconds) to remember that a neighbor platform wants an LDP session without receiving an LDP hello message from the neighbor (hold time), and the time interval between the transmission of consecutive LDP hello messages to neighbors (interval).
Discovery targeted hello	Indicates the amount of time to remember that a neighbor platform wants an LDP session when: 1. The neighbor platform is not directly connected to the router. 2. The neighbor platform has not sent an LDP hello message. This intervening interval is known as hold time. This field also indicates the time interval between the transmission of consecutive hello messages to a neighbor not directly connected to the router.
LDP for targeted sessions	Reports the parameters that have been set by the **show mpls atm-ldp bindings** command.
LDP initial/maximum backoff	Reports the parameters that have been set by the **mpls ldp backoff** command.

Related Commands

Command	Description
mpls ldp holdtime	Changes the time for which an LDP session is maintained in the absence of LDP messages from the session peer.

show mpls oam echo statistics

To display statistics about Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) echo request packets, use the **show mpls oam echo statistics** command in privileged EXEC mode.

show mpls oam echo statistics [**summary**]

Syntax Description

summary	(Optional) Displays summary information about the echo request packets (that is, the type, length, values (TLVs) version and the return codes of echo packets are not displayed).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You can use the **show mpls oam echo statistics** command to display the following:

- Currently configured TLV version for MPLS OAM operations.
- Return code distribution among the received MPLS echo reply packets.
- Statistics of sent and received MPLS echo packets, and counts of incomplete packet dispatches and timed out MPLS echo requests.

If you enter the **summary** keyword, the Echo Reply count shows all the echo reply packets, regardless of whether they are valid responses to a sent request packet. Therefore, the number of return codes will not match the number of echo reply packets received.

Examples

The following example displays sample detailed output when the **summary** keyword is not specified:

```
Router# show mpls oam echo statistics

Cisco TLV version: RFC 4379 Compliant
Return code distribution:
 !—Success (3) - 5
 B—Unlabeled output interface (9) - 0
 D—DS map mismatch (5) - 0
 f—Forward Error Correction (FEC) mismatch (10) - 0
 F—No FEC mapping (4) - 0
 I—Unknown upstream interface index (6) - 0
 L—Labeled output interface (8) - 0
 m—Unsupported TLVs (2) - 0
```

```
 M—Malformed echo request (1) - 0
 N—No label entry (11) - 0
 p—Premature termination of link-state packet (LSP) (13) - 0
 P—No receive interface label protocol (12) - 0
 U—Reserved (7) - 0
 x—No return code (0) - 0
 X—Undefined return code - 0
Echo Requests: sent (5)/received (0)/timedout (0)/unsent (0)
Echo Replies: sent (0)/received (5)/unsent (0)
```

The following example displays sample output when the **summary** keyword is specified:

```
Router# show mpls oam echo statistics summary

Cisco TLV version: RFC 4379 Compliant
Echo Requests: sent (5)/received (0)/timedout (0)/unsent (0)
Echo Replies: sent (0)/received (5)/unsent (0)
```

Table 120 describes the significant fields shown in the displays.

Table 120 show mpls oam echo statistics Field Descriptions

Field	Description
Return Code Distribution	In each line of the return code distribution, the following information is displayed: • Single-character code corresponding to the return code in the received packet (for example ! or B). • Description of the return code (for example, Success). • Value of the return code (for example, (3)). • Number of packets received with the return code (for example, 5).
sent	Number of MPLS echo request packets that the router sent.
timedout	Number of MPLS echo request packets that timed out.
received	Number of MPLS echo request packets that the router received from the network.
unsent	Number of MPLS echo requests that were not forwarded due to errors.

show mpls platform

To display platform-specific information, use the **show mpls platform** command in EXEC mode.

show mpls platform {**common** | **eompls** | **gbte-tunnels** | **reserved-vlans vlan** *vlan-id* | **statistics** [**reset**] | **vpn-vlan-mapping**}

Syntax Description

common	Displays the counters for shared code between the LAN and WAN interfaces.
eompls	Displays information about the Ethernet over Multiprotocol Label Switching (EoMPLS)-enabled interface.
gbte-tunnels	Displays information about the Multicast Multilayer Switching (MMLS) Guaranteed Bandwidth Traffic Engineering (GBTE) tunnels.
reserved-vlans vlan *vlan-id*	Displays Route Processor (RP)-reserved VLAN **show** commands; valid values are from 0 to 4095.
statistics	Displays information about the RP-control plane statistics.
reset	(Optional) Resets the statistics counters.
vpn-vlan-mapping	Displays information about the Virtual Private Network (VPN)-to-VLAN mapping table.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the counters for shared code between the LAN and WAN interfaces:

```
Router# show mpls platform common

Common MPLS counters for LAN and WAN
------------------------------------

 No. of MPLS configured LAN interfaces           = 12
 No. of cross-connect configured VLAN interfaces = 0
Router#
```

This example shows how to display the EoMPLS-enabled interface information:

```
Router# show mpls platform eompls

Interface        VLAN
GigabitEthernet  101
FastEthernet6/1  2022
Router#
```

This example shows how to display the GBTE-tunnels information:

```
Router# show mpls platform gbte-tunnels

To            From          InLbl   I/I/F kbps     Kbits    H/W Info
Router#
```

This example shows how to display the RP-reserved VLAN **show** commands:

```
Router# show mpls platform reserved-vlans vlan 1005
```

Note This example shows the output if there are no configured reserved VLANs.

This example shows how to display the information about the RP-control plane statistics:

```
Router# show mpls platform statistics

              RP MPLS Control Plane Statistics:
      ================================================
Reserved VLAN creates                    0000000001
Reserved VLAN frees                      0000000000
Reserved VLAN creation failures          0000000000
Aggregate Label adds                     0000000001
Aggregate Label frees                    0000000000
Aggregate Labels in Superman             0000000001
Feature Rsvd VLAN Reqs                   0000000000
Feature Gen Rsvd VLAN Reqs               0000000000
Feature Rsvd VLAN Free Reqs              0000000000
EoMPLS VPN# Msgs                         0000000009
EoMPLS VPN# Msg Failures                 0000000000
EoMPLS VPN# Msg Rsp Failures             0000000000
EoMPLS VPN# Set Reqs                     0000000010
EoMPLS VPN# Reset Reqs                   0000000008
FIDB mallocs                             0000000000
FIDB malloc failures                     0000000000
FIDB frees                               0000000000
EoMPLS Req mallocs                       0000000018
EoMPLS Req malloc failures               0000000000
EoMPLS Req frees                         0000000018
EoMPLS VPN# allocs                       0000000010
EoMPLS VPN# frees                        0000000008
EoMPLS VPN# alloc failures               0000000000
GB TE tunnel additions                   0000000000
GB TE tunnel label resolves              0000000000
GB TE tunnel deletions                   0000000000
GB TE tunnel changes                     0000000000
GB TE tunnel heads skips                 0000000000
gb_flow allocs                           0000000000
gb_flow frees                            0000000000
rsvp req creats                          0000000000
rsvp req frees                           0000000000
rsvp req malloc failures                 0000000000
gb_flow malloc failures                  0000000000
```

```
psb search failures                       0000000000
GB TE tunnel deleton w/o gb_flow          0000000000
errors finding slot number                0000000000
Router#
```

This example shows how to reset the RP-control plane statistics counters:

```
Router# show mpls platform statistics reset

Resetting Const RP MPLS control plane software statistics ...
GB TE tunnel additions                    0000000000
GB TE tunnel label resolves               0000000000
GB TE tunnel deletions                    0000000000
GB TE tunnel changes                      0000000000
GB TE tunnel heads skips                  0000000000
gb_flow allocs                            0000000000
gb_flow frees                             0000000000
rsvp req creats                           0000000000
rsvp req frees                            0000000000
rsvp req malloc failures                  0000000000
gb_flow malloc failures                   0000000000
psb search failures                       0000000000
GB TE tunnel deleton w/o gb_flow          0000000000
errors finding slot number                0000000000
Router#
```

This example shows how to display information about the VPN-to-VLAN mapping table:

```
Router# show mpls platform vpn-vlan-mapping

VPN#  Rsvd Vlan  IDB Created  Feature  Has agg label  In superman    EoM data
0     1025       Yes          No       No             No             No
1     0          No           No       Yes            Yes            No
Router#
```

show mpls prefix-map

Note Effective with Cisco IOS Release 12.4(20)T, the **show mpls prefix-map** command is not available in Cisco IOS software.

To display the prefix map used to assign a quality of service (QoS) map to network prefixes that match a standard IP access list, use the **show mpls prefix-map** command in privileged EXEC mode.

show mpls prefix-map [*prefix-map*]

Syntax Description

prefix-map	(Optional) Number specifying the prefix map to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was removed.

Usage Guidelines

Not entering a specific *prefix-map* argument number causes all prefix maps to be displayed.

Examples

The following is sample output from the **show mpls prefix-map** command:

```
Router# show mpls prefix-map 2

prefix-map 2 access-list 2 cos-map 2
```

Table 121 describes the fields shown in the display.

Table 121 show mpls prefix-map Field Descriptions

Field	Description
prefix-map	Unique number of a prefix map.
access-list	Unique number of an access list.
cos-map	Unique number of a QoS map.

Related Commands

Command	Description
mpls prefix-map	Configures a router to use a specified QoS map when a label destination prefix matches the specified access-list.

show mpls static binding ipv4

To display Multiprotocol Label Switching (MPLS) static label bindings, use the **show mpls static binding ipv4** command in privileged EXEC mode.

show mpls static binding ipv4 [*prefix* {*mask-length* | *mask*} | **nexthop** *address*] [**local** | **remote** [**nexthop** *address*]]

Syntax Description

prefix {*mask-length* | *mask*}	(Optional) The labels for a specific prefix.
nexthop *address*	(Optional) Specifies the labels for a next hop address.
local | **remote**	(Optional) Specifies the local (incoming) or remote (outgoing) labels to be displayed.
nexthop *address*	(Optional) Specifies the label bindings for prefixes with outgoing labels for which the specified next hop is to be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If you do not specify any optional arguments, the **show mpls static binding ipv4** command displays information about all static label bindings. Or the information can be limited to any of the following:

- Bindings for a specific prefix or mask
- Local (incoming) labels
- Remote (outgoing) labels
- Outgoing labels for a specific next hop router

Examples

In the following output, the **show mpls static binding ipv4** command with no optional arguments displays all static label bindings:

```
Router# show mpls static binding ipv4

10.0.0.0/8: Incoming label: none;
  Outgoing labels:
     10.13.0.8           explicit-null
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
     10.0.0.66              2607
```

```
10.66.0.0/16: Incoming label: 17 (in LIB)
  Outgoing labels:  None
```

In the following output, the **show mpls static binding ipv4** command displays remote (outgoing) statically assigned labels only:

```
Router# show mpls static binding ipv4 remote

10.0.0.0/8:
  Outgoing labels:
     10.13.0.8           explicit-null
10.0.0.0/8:
  Outgoing labels:
     10.0.0.66              2607
```

In the following output, the **show mpls static binding ipv4** command displays local (incoming) statically assigned labels only:

```
Router# show mpls static binding ipv4 local

10.0.0.0/8: Incoming label: 55 (in LIB)
10.66.0.0/16: Incoming label: 17 (in LIB)
```

In the following output, the **show mpls static binding ipv4** command displays statically assigned labels for prefix 10.0.0.0 / 8 only:

```
Router# show mpls static binding ipv4 10.0.0.0/8

10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
     10.0.0.66              2607
```

In the following output, the **show mpls static binding ipv4** command displays prefixes with statically assigned outgoing labels for next hop 10.0.0.66:

```
Router# show mpls static binding ipv4 10.0.0.0 8 nexthop 10.0.0.66

10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
     10.0.0.66              2607
```

Related Commands

Command	Description
mpls static binding ipv4	Binds an IPv4 prefix or mask to a local or remote label.

show mpls static binding ipv4 vrf

To display configured Multiprotocol Label Switching (MPLS) virtual routing and forwarding (VRF)-aware static bindings, use the **show mpls static binding ipv4 vrf** command in privileged EXEC mode.

show mpls static binding ipv4 vrf *vpn-name* [*prefix* {*mask-length* | *mask*} | **nexthop** *address*] [**local** | **remote** [**nexthop** *address*]]

Syntax Description

vpn-name	The static label bindings for the specified VPN routing and forwarding instance.
prefix {*mask-length* | *mask*}	(Optional) The labels for a specified prefix.
nexthop *address*	(Optional) Specifies the labels for a next hop address.
local | **remote**	(Optional) Specifies the local (incoming) or remote (outgoing) labels to be displayed.
nexthop *address*	(Optional) Specifies the label bindings for prefixes with outgoing labels for which the next hop is to be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following example displays statically assigned label bindings:

```
Router# show mpls static binding ipv4 vrf vpn100

192.168.2.2/32: (vrf: vpn100) Incoming label: 100020
Outgoing labels: None
192.168.0.29/32: Incoming label: 100003 (in LIB)
Outgoing labels: None
```

Related Commands

Command	Description
mpls static binding ipv4 vrf	Binds a prefix to a local label.

show mpls static crossconnect

To display statically configured Label Forwarding Information Database (LFIB) entries, use the **show mpls static crossconnect** command in privileged EXEC mode.

show mpls static crossconnect [*low label* [*high label*]]

Syntax Description

low label high label	(Optional) Displays the statically configured LFIB entries.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If you do not specify any label parameters, then all the configured static crossconnects are displayed.

Examples

The following output of the **show mpls static crossconnect** command shows the local and remote labels:

```
Router# show mpls static crossconnect

Local  Outgoing    Outgoing   Next Hop
label  label       interface
45     46          pos5/0     point2point
```

Table 122 describes the significant fields shown in the display.

Table 122 show mpls static crossconnect Field Descriptions

Field	Description
Local label	Label assigned by this router.
Outgoing label	Label assigned by the next hop.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of next hop router's interface that is connected to this router's outgoing interface.

Related Commands

Command	Description
mpls static crossconnect	Configures an LFIB entry for the specified incoming label and outgoing interface.

show mpls traffic tunnel backup

To display information about the backup tunnels that are currently configured, use the **show mpls traffic tunnel backup** command in user EXEC or privileged EXEC mode.

show mpls traffic tunnel backup tunnel*tunnel-id*

Syntax Description

tunnel*tunnel-id*	Tunnel ID of the backup tunnel for which you want to display information.

Command Default

Information about currently configured backup tunnels is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Examples

The following is sample output from the **show mpls traffic tunnel backup tunnel** *tunnel-id* command:

```
Router# show mpls traffic tunnel backup tunnel1000

Tunnel1000          Dest: 10.0.0.9        State: Up
any-pool cfg 100 inuse 0 num_lsps 0
     protects: ATM0.1
```

Table 123 describes the significant fields shown in the display.

Table 123 show mpls traffic tunnel backup Field Descriptions

Field	Description
Tunnel	Tunnel ID of the backup tunnel for which this information is being displayed.
Dest	IP address of the destination of the backup tunnel.
State	State of the backup tunnel. Valid values are Up, Down, or Admin-down.
any-pool	Pool from which bandwidth is acquired. Valid values are any-pool, global-pool, and sub-pool.
cfg	Amount of bandwidth configured for that pool.
inuse	Amount of bandwidth currently being used.

Table 123 show mpls traffic tunnel backup Field Descriptions (continued)

Field	Description
num_lsps	Number of label-switched paths (LSPs) being protected.
protects	The protected interfaces that are using this backup tunnel.

Related Commands

Command	Description
tunnel mpls traffic-eng backup-bw	Specifies what types of LSPs can use a backup tunnel, whether the backup tunnel should provide bandwidth protection, and if so, how much.

show mpls traffic-eng autoroute

To display tunnels announced to the Interior Gateway Protocol (IGP), including interface, destination, and bandwidth, use the **show mpls traffic-eng autoroute** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng autoroute

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The enhanced shortest path first (SPF) calculation of the IGP has been modified so that it uses traffic engineering tunnels. This command shows which tunnels IGP is currently using in its enhanced SPF calculation (that is, which tunnels are up and have autoroute configured).

Examples

The following is sample output from the **show mpls traffic-eng autoroute** command.

Note that the tunnels are organized by destination. All tunnels to a destination carry a share of the traffic tunneled to that destination.

```
Router# show mpls traffic-eng autoroute

MPLS TE autorouting enabled
  destination 0002.0002.0002.00 has 2 tunnels
    Tunnel1021 (traffic share 10000, nexthop 10.2.2.2, absolute metric 11)
    Tunnel1022 (traffic share 3333, nexthop 10.2.2.2, relative metric -3)
  destination 0003.0003.0003.00 has 2 tunnels
    Tunnel1032 (traffic share 10000, nexthop 172.16.3.3)
    Tunnel1031 (traffic share 10000, nexthop 172.16.3.3, relative metric -1)
```

Table 124 describes the significant fields shown in the display.

Table 124 show mpls traffic-eng autoroute Field Descriptions

Field	Description
MPLS TE autorouting enabled	IGP automatically routes traffic into tunnels.
destination	MPLS traffic engineering tailend router system ID.
traffic share	A factor based on bandwidth, indicating how much traffic this tunnel should carry, relative to other tunnels, to the same destination. If two tunnels go to a single destination, one with a traffic share of 200 and the other with a traffic share of 100, the first tunnel carries two-thirds of the traffic.
nexthop	MPLS traffic engineering tailend IP address of the tunnel.
absolute metric	MPLS traffic engineering metric with mode absolute of the tunnel.
relative metric	MPLS traffic engineering metric with mode relative of the tunnel.

Related Commands

Command	Description
show isis mpls traffic-eng tunnel	Displays information about tunnels considered in the IS-IS next hop calculation.
tunnel mpls traffic-eng autoroute announce	Causes the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.
tunnel mpls traffic-eng autoroute metric	Specifies the MPLS traffic engineering tunnel metric that the IGP enhanced SPF calculation will use.

show mpls traffic-eng auto-tunnel mesh

To display the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers, use the **show mpls traffic-eng auto-tunnel mesh** command in user EXEC mode or privileged EXEC mode.

show mpls traffic-eng auto-tunnel mesh

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following is output from the **show mpls traffic-eng auto-tunnel mesh** command that shows the cloned mesh tunnel interfaces for autotemplate1 and shows the range of mesh tunnel interface numbers. Information for only one autotemplate is displayed because only one autotemplate was configured.

```
Router# show mpls traffic-eng auto-tunnel mesh

Auto-Template1:

 Using access-list 1 to clone the following tunnel interfaces:

  Destination  Interface
  -----------  ---------
  10.2.2.2     Tunnel64336
  10.3.3.3     Tunnel64337

Mesh tunnel interface numbers: min 64336 max 65337
```

Table 125 describes the significant fields shown in the display.

Table 125 show mpls traffic-eng auto-tunnel mesh Field Descriptions

Field	Description
Auto-Template1	Name of the autotemplate.
Destination	Destination addresses for the mesh tunnel interface cloned from access list 1.

Table 125 show mpls traffic-eng auto-tunnel mesh Field Descriptions (continued)

Field	Description
Interface	Mesh tunnel interfaces cloned from access list 1.
min 64336 max 65337	Range of mesh tunnel interface numbers for this Auto-Template1—minimum (64336) and maximum (65337).

Related Commands

Command	Description
interface auto-template	Creates the template interface.
mpls traffic-eng auto-tunnel mesh tunnel-num	Configures the range of mesh tunnel interface numbers.

show mpls traffic-eng destination list

To display an Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) destination list, use the **show mpls traffic-eng destination list** command in user EXEC or privileged EXEC configuration mode.

show mpls traffic-eng destination list [**name** *destination-list-name* | **identifier** *destination-list-identifier*]

Syntax Description

name *destination-list-name*	(Optional) Specifies the name of a destination list.
identifier *destination-list-identifier*	(Optional) Specifies the number of a destination list.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

This command displays the information about any destination lists configured for an MPLS TE P2MP configuration.

Examples

The following example displays information about a destination list:

```
Router# show mpls traffic-eng destination-list

Destination list: name p2mp-list1
    ip 10.3.3.3 path-option 1 dynamic
    ip 10.4.4.4 path-option 15 explicit identifier 4
    ip 10.5.5.5 path-option 2 explicit name r1-r2-r4-r5
```

Table 126 describes the significant fields shown in the display.

Table 126 show mpls traffic-eng destination-list Field Descriptions

Field	Description
Destination list	The name of the destination list.
ip	The IP address of the path's destination.
path-option	Information about the dynamic or explicit path.

Related Commands

Command	Description
mpls traffic-eng destination-list	Creates a destination list for MPLS Point-to-Multipoint Traffic Engineering.

show mpls traffic-eng fast-reroute database

To display the contents of the Fast Reroute (FRR) database, use the **show mpls traffic-eng fast-reroute database** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng fast-reroute database [*network* [*mask* | *masklength*] | **labels** *low label* [*-high label*] | **interface** *ifname* [**backup-interface** *ifname*] | **backup-interface** *ifname*] [**state** {**active** | **ready** | **partial** | **complete**}] [**role** {**head** | **middle**}] [**detail**] [**vrf** *name*]

Syntax Description

network	(Optional) IP address of the destination network. This functions as the prefix of the FRR rewrite.
mask	(Optional) Bit combination indicating the portion of the IP address that is being used for the subnet address.
masklength	(Optional) Number of bits in mask of destination.
labels	(Optional) Shows only database entries that possess in-labels (local labels) assigned by this router. You specify either a starting value or a range of values.
low label	(Optional) Starting label value or lowest value in the range.
-high label	(Optional) Highest label value in the range.
interface	(Optional) Shows only database entries related to the primary outgoing interface.
ifname	(Optional) Name of the primary outgoing interface.
backup-interface	(Optional) Shows only database entries related to the backup outgoing interface.
ifname	(Optional) Name of the backup outgoing interface.
state	(Optional) Shows entries that match one of four possible states: active, ready, partial, or complete.
active	The FRR rewrite has been put into the forwarding database (where it can be placed onto appropriate incoming packets).
ready	The FRR rewrite has been created, but has not yet been moved into the forwarding database.
partial	State before the FRR rewrite has been fully created; its backup routing information is still incomplete.
complete	State after the FRR rewrite has been assembled: it is either ready or active.
role	(Optional) Shows entries associated either with the tunnel head or tunnel midpoint.
head	Entry associated with tunnel head.
middle	Entry associated with tunnel midpoint.
detail	(Optional) Shows long-form information: LFIB-FRR total number of clusters, groups, and items in addition to the short-form information of prefix, label and state.
vrf *name*	(Optional) Shows entries for a Virtual Private Network (VPN) routing/forwarding instance.

Command Default The contents of the FRR database are not displayed.

Command Modes User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Catalyst 6000 series with the SUP720 processor.
12.2(28)SB	This command was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The ouptut was updated to display Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) information.

Examples The following example shows output from the **show mpls traffic-eng fast-reroute database** command at a tunnel head link:

```
Router# show mpls traffic-eng fast-reroute database 10.0.0.0

Tunnel head fast reroute information:

Prefix       Tunnel  In-label  Out intf/label  FRR intf/label  Status
10.0.0.0/16   Tu111   Tun hd    PO0/0:Untagged  Tu4000:16       ready
10.0.0.0/16   Tu449   Tun hd    PO0/0:Untagged  Tu4000:736      ready
10.0.0.0/16   Tu314   Tun hd    PO0/0:Untagged  Tu4000:757      ready
10.0.0.0/16   Tu313   Tun hd    PO0/0:Untagged  Tu4000:756      ready
```

Table 127 describes the significant fields shown in the display.

Table 127 show mpls traffic-eng fast-reroute database Field Descriptions

Field	Description
Prefix	Address to which packets with this label are going.
Tunnel	Tunnel's identifying number.
In-label	Label advertised to other routers to signify a particular prefix. The value "Tun hd" occurs when no such label has been advertised.

Table 127 show mpls traffic-eng fast-reroute database Field Descriptions (continued)

Field	Description
Out intf/label	Out interface—short name of the physical interface through which traffic goes to the protected link. Out label: • At a tunnel head, this is the label advertised by the tunnel destination device. The value "Untagged" occurs when no such label has been advertised. • At tunnel midpoints, this is the label selected by the next hop device. The "Pop Tag" value occurs when the next hop is the tunnel's final hop.
FRR intf/label	Fast Reroute interface—the backup tunnel interface. Fast Reroute label: • At a tunnel head, this is the label selected by the tunnel tail to indicate the destination network. The value "Untagged" occurs when no such label has been advertised. • At tunnel midpoints, this has the same value as the Out Label.
Status	State of the rewrite: partial, ready, or active. (These terms are defined above in the "Syntax Description" section).

The following example shows output from the **show mpls traffic-eng fast-reroute database** command with the **labels** keyword specified at a midpoint link:

```
Router# show mpls traffic-eng fast-reroute database labels 250-255

Tunnel head fast reroute information:
Prefix   Tunnel   In-label   Outintf/label   FRR intf/label   Status

LSP midpoint frr information:

LSP identifier          In-label   Out intf/label  FRR intf/label  Status
10.110.0.10 229 [7334] 255        PO0/0:694       Tu4000:694      active
10.110.0.10 228 [7332] 254        PO0/0:693       Tu4000:693      active
10.110.0.10 227 [7331] 253        PO0/0:692       Tu4000:692      active
10.110.0.10 226 [7334] 252        PO0/0:691       Tu4000:691      active
10.110.0.10 225 [7333] 251        PO0/0:690       Tu4000:690      active
10.110.0.10 224 [7329] 250        PO0/0:689       Tu4000:689      active
```

The following example shows output from the **show mpls traffic-eng fast-reroute database** command with the **detail** keyword included at a tunnel head link:

```
Router# show mpls traffic-eng fast-reroute database 10.0.0.0. detail

LFIB FRR Database Summary:
  Total Clusters:      2
  Total Groups:        2
  Total Items:         789
Link 10:PO5/0 (Down, 1 group)
  Group 51:PO5/0->Tu4000 (Up, 779 members)
    Prefix 10.0.0.0/16, Tu313, active
      Input label Tun hd, Output label PO0/0:773, FRR label Tu4000:773
    Prefix 10.0.0.0/16, Tu392, active
      Input label Tun hd, Output label PO0/0:775, FRR label Tu4000:775
    Prefix 10.0.0.0/16, Tu111, active
      Input label Tun hd, Output label PO0/0:16, FRR label Tu4000:16
    Prefix 10.0.0.0/16, Tu394, active
```

```
Input label Tun hd, Output label PO0/0:774, FRR label Tu4000:774
```

Table 128 describes the significant fields when the **detail** keyword is used.

Table 128 show mpls traffic-eng fast-reroute database with detail Keyword Field Descriptions

Field	Description
Total Clusters	A cluster is the physical interface upon which Fast Reroute link protection has been enabled.
Total Groups	A group is a database record that associates the link-protected physical interface with a backup tunnel. A cluster (physical interface) therefore can have one or more groups. For example, the cluster Ethernet4/0/1 is protected by backup Tunnel1 and backup Tunnel2, and so has two groups.
Total Items	An item is a database record that associates a rewrite with a group. A group therefore can have one or more items.
Link 10:PO5/0 (Down, 1 group)	This describes a cluster (physical interface): • "10" is the interface's unique IOS-assigned ID number. • ":" is followed by the interface's short name. • Parentheses contain the operating state of the interface (Up or Down) and the number of groups associated with it.
Group 51:PO5/0->Tu4000 (Up, 779 members)	This describes a group: • "51" is the ID number of the backup interface. • ":" is followed by the group's physical interface short name. • "->" is followed by the backup tunnel interface short name. • Parentheses contain the operating state of the tunnel interface (Up or Down) and the number of items—also called "members"— associated with it.

MPLS Traffic Engineering Point-to-Multipoint Fast Reroute Information

The following example shows MPLS TE P2MP information as part of the command output.

```
Router> show mpls traffic-eng fast-reroute database

P2P Headend FRR information:
Protected tunnel              In-label Out intf/label   FRR intf/label   Status
---------------------------   -------- --------------   --------------   ------
Tunnel1                       Tun hd   Et0/1:20         Tu777:20         ready

P2P LSP midpoint frr information:
LSP identifier                In-label Out intf/label   FRR intf/label   Status
---------------------------   -------- --------------   --------------   ------
```

```
P2MP Sub-LSP FRR information:
Sub-LSP identifier
src_lspid[subid]->dst_tunid    In-label Out intf/label   FRR intf/label   Status
---------------------------    -------- --------------   --------------   ------
10.1.1..201_1[1]->10.1.1..203_22   Tun hd   Et0/0:20         Tu666:20         ready
10.1.1..201_1[2]->10.1.1..206_22   Tun hd   Et0/0:20         Tu666:20         ready
10.1.1..201_1[3]->10.1.1..213_22   Tun hd   Et0/0:20         Tu666:20         ready
```

Table 129 describes the significant fields shown in the display.

Table 129 show mpls traffic-eng fast-reroute database Point-to-Multipoint Field Descriptions

Field	Description
Sub-LSP identifier src_lspid[subid]->dst_tunid	The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address.

The detail keyword provides more information about the P2MP LSPs:

```
Router# show mpls traffic-eng fast-reroute database detail

FRR Database Summary:
     Number of protected interfaces: 1
     Number of protected tunnels: 2
     Number of backup tunnels: 1
     Number of active interfaces: 0
P2MP Sub-LSPs:
   Tun ID: 1, LSP ID: 9, Source: 10.2.0.1
   Destination: 10.2.5.3, Subgroup ID: 19
   State        : Ready
   InLabel      : Tunnel Head
   OutLabel     : Se6/0:16
   FRR OutLabel : Tu100:16
```

Command	Description
show mpls traffic-eng fast-reroute log reroutes	Displays contents of Fast Reroute event log.

show mpls traffic-eng fast-reroute log reroutes

To display the contents of the Fast Reroute event log, use the **show mpls traffic-eng fast-reroute log reroutes** command in user EXEC mode.

show mpls traffic-eng fast-reroute log reroutes

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

user EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Catalyst 6000 series with the SUP720 processor.
12.2(28)SB	This command was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows output from the **show mpls traffic-eng fast-reroute log reroutes** command:

```
Router# show mpls traffic-eng fast-reroute log reroutes

When      Interface  Event   Rewrites  Duration  CPU msecs  Suspends  Errors
00:27:39  PO0/0      Down    1079      30 msecs  30         0         0
00:27:35  PO0/0      Up      1079      40 msecs  40         0         0
```

Table 130 describes significant fields shown in the display.

Table 130 show mpls traffic-eng fast-reroute log reroutes Field Descriptions

Field	Description
When	Indicates how long ago the logged event occurred (before this line was displayed on your screen). Displayed as hours, minutes, seconds.
Interface	The physical or tunnel interface where the logged event occurred.
Event	The change to Up or Down by the affected interface.
Rewrites	Total number of reroutes accomplished because of this event.
Duration	Time elapsed during the rerouting process, in milliseconds.
CPU msecs	CPU time spent processing those reroutes, in milliseconds. (This is less than or equal to the Duration value).

Table 130 show mpls traffic-eng fast-reroute log reroutes Field Descriptions (continued)

Field	Description
Suspends	Number of times that reroute processing for this event was interrupted to let the CPU handle other tasks.
Errors	Number of unsuccessful reroute attempts.

show mpls traffic-eng forwarding-adjacency

To display traffic engineering (TE) tunnels that are advertised as links in an Interior Gateway Protocol (IGP) network, use the **show mpls traffic-eng forwarding-adjacency** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng forwarding-adjacency [*ip-address*]

Syntax Description

ip-address	(Optional) Destination address for forwarding adjacency tunnels.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.0(16)ST	This command was integrated into Cisco IOS Release 12.0(16)ST.
12.2(18)S	This command was integrated into Cisco IOS Release 2.2(18)S.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show mpls traffic-eng forwarding-adjacency** command to display information about tunnels configured with the **tunnel mpls traffic-eng forwarding-adjacency** command.

Examples

The following is sample output from the **show mpls traffic-eng forwarding-adjacency** command:

```
Router# show mpls traffic-eng forwarding-adjacency

  destination 0168.0001.0007.00 has 1 tunnels
    Tunnel7     (traffic share 100000, nexthop 192.168.1.7)
                (flags:Announce Forward-Adjacency, holdtime 0)

Router# show mpls traffic-eng forwarding-adjacency 192.168.1.7

  destination 0168.0001.0007.00 has 1 tunnels
    Tunnel7     (traffic share 100000, nexthop 192.168.1.7)
                (flags:Announce Forward-Adjacency, holdtime 0)
```

Related Commands

Command	Description
debug mpls traffic-eng forwarding-adjacency	Displays debug messages for traffic engineering forwarding adjacency events.
tunnel mpls traffic-eng forwarding-adjacency	Advertises a TE tunnel as a link in an IGP network.

show mpls traffic-eng forwarding path-set

To display the sublabel switched paths (sub-LSPs) that originate from the headend router, use the **show mpls traffic-eng forwarding path-set** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng forwarding path-set [**brief** | **detail**]

Syntax Description

brief	(Optional) Displays information about the sub-LSPs in a table format.
detail	(Optional) Displays detailed information about the sub-LSPs.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example displays information about the sub-LSPs in a summary format, including the number of sub-LSPs and the number of paths from the headend router.

```
Router> show mpls traffic-eng forwarding path-set

ID       Input I/F  LSPID  InLabel  PathCnt  subLSPCnt
----     ---------  -----  -------  -------  ---------
9F000001 Tu22       1      none     2        6
```

The following example shows six sub-LSPs originating at the headend router and going to different destinations. All the sub-LSPs belong to the same path set, which is a collection of paths. The path set is given a unique ID, which is shown in the PSID column of the example:

```
Router# show mpls traffic-eng forwarding path-set brief

Sub-LSP Identifier
src_lspid[subid]->dst_tunid              InLabel Next Hop      I/F    PSID
--------------------------               ------- ------------- ------ ----
10.1.1.201_1[1]->10.1.1.203_22             none    10.0.0.205    Et0/0  9F000001
10.1.1.201_1[2]->10.1.1.206_22             none    10.0.0.205    Et0/0  9F000001
10.1.1.201_1[3]->10.1.1.213_22             none    10.0.0.205    Et0/0  9F000001
10.1.1.201_1[4]->10.1.1.214_22             none    10.0.1.202    Et0/1  9F000001
10.1.1.201_1[5]->10.1.1.216_22             none    10.0.1.202    Et0/1  9F000001
10.1.1.201_1[6]->10.1.1.217_22             none    10.0.1.202    Et0/1  9F000001
```

The **show mpls traffic-eng forwarding path-set detail** command shows more information about the sub-LSPs that originate from the headend router. For example:

```
Router# show mpls traffic-eng forwarding path-set detail

LSP: Source: 10.1.0.1, TunID: 100, LSPID: 7
  Destination: 10.2.0.1, P2MP Subgroup ID: 1
    Path Set ID: 0x30000001
    OutLabel : Serial2/0, 16
    Next Hop : 10.1.3.2
```

```
    FRR OutLabel : Tunnel666, 16

LSP: Source: 10.1.0.1, TunID: 100, LSPID: 7
Destination: 10.3.0.1, P2MP Subgroup ID: 2
  Path Set ID: 0x30000001
  OutLabel : Serial2/0, 16
  Next Hop : 10.1.3.2
  FRR OutLabel : Tunnel666, 16
```

Table 131 describes the significant fields shown in the display.

Table 131 show mpls traffic-eng forwarding path-set Field Descriptions

Field	Description
ID	Path set ID.
Input I/F	The ID assigned to the tunnel that the sub-LSPs use.
LSPID	Sub-LSP ID.
InLabel	MPLS label in the input interface.
PathCnt	Number of paths from the headend router.
subLSPCnt	Number of sub-LSPS from the headend router.
Sub-LSP Identifier src_lspid[subid]->dst_tunid	The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address.
Next Hop	Next-hop router.
I/F	The interface that the sub-LSPs use.
PSID	Path set ID.
Source	IP address of the headend router.
TunID	The ID assigned to the tunnel that the sub-LSPs use.
Destination	IP address of the destination router.
P2MP Subgroup ID	A consectutive number assigned to each sub-LSP.
Path Set ID	Path set ID.
OutLabel	The interface from which the label exits and the MPLS label that exits the interface.
FRR OutLabel	The tunnel from which the label exits and the MPLS label that exits the tunnel.

Related Commands

Command	Description
ip path-option	Species an explicit or dynamic path option for a particular destination address in a destination list

show mpls traffic-eng forwarding statistics

To display information about Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-pultipoint (P2MP) paths and sublabel switched paths (sub-LSPs), use the **show mpls traffic-eng forwarding statistics** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng forwarding statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example displays informtion about MPLS TE P2MP paths and sub-LSPs:

```
Router# show mpls traffic-eng forwarding statistics

TE P2MP:

Statistics:
    Path Set Creation:            2
    Path Set Deletion:            0
    Input Label Allocation for Path Sets:  2
    Input Label Free:             0
    Current Label Allocated:      2
    PSI Nodes Allocated:          2
    PSI Nodes Freed:              0
    Add sub-LSP to Path Set:      5
    Delete sub-LSP from Path Set  0 (prune: 0, flush: 0)
    Update Path for FRR:          4

  Failures:
    None
```

Table 132 describes the significant fields shown in the display.

Table 132 show mpls traffic-eng forwarding statistics Field Descriptions

Field	Description
Path Set Creation	Number of path sets created.
Path Set Deletion	Number of path sets deleted.
Input Label Allocation for Path Sets	Number of input labels allocated for the path sets.
Input Label Free	Number of free input labels.
Current Label Allocated	Number of labels allocated for forwarding.

Table 132 show mpls traffic-eng forwarding statistics Field Descriptions (continued)

Field	Description
PSI Nodes Allocated	Number of path set nodes allocated.
PSI Nodes Freed	Number of path set nodes freed
Add sub-LSP to Path Set	Number of sub-LSPs in the path set.
Delete sub-LSP from Path Set	Number of sub-LSPs removed from the path set, either by pruning or flushing.
Update Path for FRR	Number of paths updated for fast reroute.
Failures	Number of path set failures

Related Commands

Command	Description
show mpls traffic-eng forwarding path-set	Display the sub-LSPs that originate from the headend router.

show mpls traffic-eng link-management admission-control

To show which tunnels were admitted locally and their parameters (such as, priority, bandwidth, incoming and outgoing interface, and state), use the **show mpls traffic-eng link-management admission-control** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng link-management admission-control [*interface-name*]

Syntax Description

interface-name	(Optional) Displays only tunnels that were admitted on the specified interface.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed. The BW field now shows bandwidth in kBps, and it is followed by the status (reserved or held) of the bandwidth.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show mpls traffic-eng link-management admission-control** command:

```
Router # show mpls traffic-eng link-management admission-control

System Information::
    Tunnels Count:       4
    Tunnels Selected:    4
TUNNEL ID              UP IF     DOWN IF  PRIORITY STATE           BW (kbps)
10.106.0.6 1000_1      AT1/0.2   -        0/0      Resv Admitted   0
10.106.0.6 2000_1      Et4/0/1   -        1/1      Resv Admitted   0
10.106.0.6 1_2         Et4/0/1   Et4/0/2  1/1      Resv Admitted   3000       R
10.106.0.6 2_2         AT1/0.2   AT0/0.2  1/1      Resv Admitted   3000       R
```

Table 133 describes the significant fields shown in the display.

Table 133 show mpls traffic-eng link-management admission-control Field Descriptions

Field	Description
Tunnels Count	Total number of tunnels admitted.
Tunnels Selected	Number of tunnels to be displayed.
TUNNEL ID	Tunnel identification.

Table 133 show mpls traffic-eng link-management admission-control Field Descriptions

Field	Description
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.
PRIORITY	Setup priority of the tunnel followed by the hold priority.
STATE	Admission status of the tunnel.
BW (kbps)	Bandwidth of the tunnel (in kBps). If an “R” follows the bandwidth number, the bandwidth is reserved. If an “H” follows the bandwidth number, the bandwidth is temporarily being held for a path message.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Displays local link information that MPLS traffic engineering link management is currently flooding into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.
show mpls traffic-eng link-management igp-neighbors	Displays IGP neighbors.
show mpls traffic-eng link-management interfaces	Displays per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Displays a summary of link management information.

show mpls traffic-eng link-management advertisements

To display local link information that Multiprotocol Label Switching (MPLS) traffic engineering link management is flooding into the global traffic engineering topology, use the **show mpls traffic-eng link-management advertisements** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng link-management advertisements

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The output was enhanced to show Internet Gateway Protocol (IGP) recovery status provided by the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples

The following is sample output from the **show mpls traffic-eng link-management advertisements** command:

```
Router# show mpls traffic-eng link-management advertisements

Flooding Status:     ready
Configured Areas:    1
IGP Area[1] ID:: isis level-1
  System Information::
    Flooding Protocol:   ISIS
  Header Information::
    IGP System ID:       0001.0000.0001.00
    MPLS TE Router ID:   10.106.0.6
    Flooded Links:       1
  Link ID:: 0
    Link IP Address:     10.1.0.6
    IGP Neighbor:        ID 0001.0000.0001.02
    Admin. Weight:       10
    Physical Bandwidth:  10000 kbits/sec
    Max Reservable BW:   5000 kbits/sec
    Downstream::
      Reservable Bandwidth[0]:       5000 kbits/sec
      Reservable Bandwidth[1]:       2000 kbits/sec
      Reservable Bandwidth[2]:       2000 kbits/sec
      Reservable Bandwidth[3]:       2000 kbits/sec
      Reservable Bandwidth[4]:       2000 kbits/sec
      Reservable Bandwidth[5]:       2000 kbits/sec
```

```
    Reservable Bandwidth[6]:       2000 kbits/sec
    Reservable Bandwidth[7]:       2000 kbits/sec
  Attribute Flags:     0x00000000
```

Table 134 describes the significant fields shown in the display.

Table 134 show mpls traffic-eng link-management advertisements Field Descriptions

Field	Description
Flooding Status	Status of the link management flooding system.
Configured Areas	Number of the Interior Gateway Protocol (IGP) areas configured.
IGP Area [1] ID	Name of the first IGP area.
Flooding Protocol	IGP that is flooding information for this area.
IGP System ID	Identification that IGP flooding uses in this area to identify this node.
MPLS TE Router ID	MPLS traffic engineering router ID.
Flooded Links	Number of links that are flooded in this area.
Link ID	Index of the link that is being described.
Link IP Address	Local IP address of this link.
IGP Neighbor	IGP neighbor on this link.
Admin. Weight	Administrative weight associated with this link.
Physical Bandwidth	Link bandwidth capacity (in kBps).
Max Reservable BW	Amount of reservable bandwidth (in kBps) on this link.
Reservable Bandwidth	Amount of bandwidth (in kBps) that is available for reservation.
Attribute Flags	Attribute flags of the link are being flooded.

The following is sample output from the **show mpls traffic-eng link-management advertisements** command with the enhanced output, which shows the “IGP recovering” status, from the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature:

```
Router# show mpls traffic-eng link-management advertisements

show mpls traffic-eng link-management advertisements
Flooding Status:      ready (IGP recovering)
Configured Areas:     1
IGP Area[1] ID::  ospf  area nil
  System Information::
    Flooding Protocol:    OSPF
  Header Information::
```

Table 135 describes the significant fields shown in the display.

Table 135 show mpls traffic-eng link-management advertisements Field Descriptions

Field	Description
Flooding Status	Status of the link management flooding system. The notation (IGP recovering) indicates that flooding cannot be determined because an IP routing process restart is in progress.
Configured Areas	Number of the IGP areas configured.

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.
show mpls traffic-eng link-management igp-neighbors	Displays IGP neighbors.
show mpls traffic-eng link-management interfaces	Displays per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Displays a summary of link management information.

show mpls traffic-eng link-management bandwidth-allocation

To display current local link information, use the **show mpls traffic-eng link-management bandwidth-allocation** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng link-management bandwidth-allocation [*interface-name* | **summary** [*interface-name*]]

Syntax Description

interface-name	(Optional) Displays only tunnels that were admitted on the specified interface.
summary *interface-name*	(Optional) Displays bandwidth usage forthe specified interfaces.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	The **summary** *interface-name* keyword-argument combination was added.

Usage Guidelines

Advertised information might differ from the current information, depending on how flooding was configured.

Examples

Interface Example

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation** command for a specified interface:

```
Router# show mpls traffic-eng link-management bandwidth-allocation Et4/0/1

System Information::
    Links Count:         2
    Bandwidth Hold Time: max. 15 seconds
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      BW Descriptors:      1
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
      Outbound Admission:  allow-if-room
```

```
  Admin. Weight:       10 (IGP)
  IGP Neighbor Count:  1
  Up Thresholds:       15 30 45 60 75 80 85 90 95 96 97 98 99 100 (default)
  Down Thresholds:     100 99 98 97 96 95 90 85 80 75 60 45 30 15 (default)
Downstream Bandwidth Information (kbits/sec):
  KEEP PRIORITY     BW HELD  BW TOTAL HELD   BW LOCKED  BW TOTAL LOCKED
              0           0              0           0                0
              1           0              0        3000             3000
              2           0              0           0             3000
              3           0              0           0             3000
              4           0              0           0             3000
              5           0              0           0             3000
              6           0              0           0             3000
              7           0              0           0             3000
```

Table 136 describes the significant fields shown in the display.

Table 136 show mpls traffic-eng link-management bandwidth-allocation Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS traffic engineering.
Bandwidth Hold Time	Amount of time that bandwidth can be held.
Link ID	Interface name and IP address of the link being described.
Physical Bandwidth	Link bandwidth capacity (in bits per second).
Max Reservable BW	Amount of reservable bandwidth on this link.
BW Descriptors	Number of bandwidth allocations on this link.
MPLS TE Link State	Status of the link's MPLS traffic engineering-related functions.
Inbound Admission	Link admission policy for incoming tunnels.
Outbound Admission	Link admission policy for outgoing tunnels.
Admin. Weight	Link administrative weight.
IGP Neighbor Count	List of the IGP neighbors directly reachable over this link.
Up Thresholds	Link's bandwidth thresholds for allocations.
Down Thresholds	Link's bandwidth thresholds for deallocations.
KEEP PRIORITY	Priority levels for the link's bandwidth allocations.
BW HELD	Amount of bandwidth (in kBps) temporarily held at this priority for path messages.
BW TOTAL HELD	Bandwidth held at this priority and those above it.
BW LOCKED	Amount of bandwidth reserved at this priority.
BW TOTAL LOCKED	Bandwidth locked at this priority and those above it.

Summary Example for Regular Traffic Engineering (TE) (or Russian Dolls Model [RDM] DiffServ-aware TE) with Multiple Interfaces

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation summary** command for all the configured interfaces:

```
Router# show mpls traffic-eng link-management bandwidth-allocation summary

  interface     Intf Max    Intf Avail  Sub Max     Sub Avail
                kbps        kbps        kbps        kbps
```

```
  Et0/0         47000       42500       42000       40500
  Et1/0         7500        7500        0           0
```

Table 137 describes the significant fields shown in the display.

Table 137 show mpls traffic-eng link-management bandwidth-allocation summary Field Descriptions

Field	Description
interface	Name of the interface.
Intf Max	Maximum amount of bandwidth (in kbps) available on the interface.
Intf Avail	Amount of bandwidth (in kbps) currently available on the interface.
Sub Max	Maximum amount of bandwidth (in kbps) available in the subpool.
Sub Avail	Amount of bandwidth (in kbps) currently available in the subpool.

Summary Example for Regular Traffic Engineering (TE) (or Russian Dolls Model [RDM] DiffServ-aware TE) with a Single Interface

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation summary** command for one configured interface:

```
Router# show mpls traffic-eng link-management bandwidth-allocation summary Ethernet0/0

interface     Intf Max    Intf Avail  Sub Max     Sub Avail
                kbps        kbps        kbps        kbps
  Et0/0         47000       42500       42000       40500
```

See Table 137 for an explanation of the preceding fields.

Summary Example with Specified Interface for Maximum Allocation Model (MAM) DS-TE

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation summary** command for all the configured interfaces:

```
Router# show mpls traffic-eng link-management bandwidth-allocation summary

  interface     Intf Max    BC0 Max     BC0 Avail   BC1 Max     BC1 Avail
                kbps        kbps        kbps        kbps        kbps
  Et0/0         45000       40000       37000       30000       28500
  Et1/0         0           0           0           0           0
```

Table 138 describes the significant fields shown in the display.

Table 138 show mpls traffic-eng link-management bandwidth-allocation summary Field Descriptions

Field	Description
interface	Name of the interface.
Intf Max	Maximum amount of bandwidth (in kbps) available on the interface.
BC0 Max	Maximum amount of bandwidth (in kbps) available in the global pool.

Table 138 show mpls traffic-eng link-management bandwidth-allocation summary Field Descriptions (continued)

Field	Description
BC0 Avail	Amount of bandwidth (in kbps) currently available in the global pool.
BC1 Max	Maximum amount of bandwidth (in kbps) available in the subpool.
BC1 Avail	Amount of bandwidth (in kbps) currently available in the subpool.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management igp-neighbors	Displays IGP neighbors.
show mpls traffic-eng link-management interfaces	Displays per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Displays a summary of link management information.

show mpls traffic-eng link-management igp-neighbors

To show Interior Gateway Protocol (IGP) neighbors, use the **show mpls traffic-eng link-management igp-neighbors** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng link-management igp-neighbors [*igp-id* [**isis** *isis-address* | **ospf** *ospf-id*] | **ip** *A.B.C.D*]

Syntax Description

igp-id	(Optional) Displays the IGP neighbors that are using a specified IGP identification.
isis *isis-address*	(Optional) Displays the specified IS-IS neighbor when you display neighbors by IGP ID.
ospf *ospf-id*	(Optional) Displays the specified OSPF neighbor when you display neighbors by IGP ID.
ip *A.B.C.D*	(Optional) Displays the IGP neighbors that are using a specified IGP IP address.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show mpls traffic-eng link-management igp-neighbors** command:

```
Router# show mpls traffic-eng line-management igp-neighbors

Link ID::  Et0/2
    Neighbor ID:  0000.0024.0004.02 (area: isis level-1, IP: 10.0.0.0)
Link ID::  PO1/0/0
    Neighbor ID:  0000.0026.0001.00 (area: isis level-1, IP: 172.16.1.2)
```

Table 139 describes the significant fields shown in the display.

Table 139 show mpls traffic-eng link-management igp-neighbors Field Descriptions

Field	Description
Link ID	Link by which the neighbor is reached.
Neighbor ID	IGP identification information for the neighbor.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.
show mpls traffic-eng link-management interfaces	Displays per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Displays a summary of link management information.

show mpls traffic-eng link-management interfaces

To display interface resource and configuration information, use the **show mpls traffic-eng link-management interfaces** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng link-management interfaces [*interface-name*]

Syntax Description

interface-name	(Optional) Displays information only for the specified interface.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	The command output was enhanced to display the Shared Risk Link Group (SRLG) membership of links.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to display resource and configuration information for all configured interfaces.

Examples

The following is sample output from the **show mpls traffic-eng link-management interfaces** command:

```
Router# show mpls traffic-eng link-management interfaces Et4/0/1

System Information::
    Links Count:         2
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      IGP Neighbor:        ID 0001.0000.0001.02, IP 10.0.0.0 (Up)
      Flooding Status for each configured area [1]:
      IGP Area[1]: isis level-1: flooded
```

The following is sample output from the **show mpls traffic-eng link-management interfaces** command when SRLGs are configured:

```
Router# show mpls traffic-eng link-management interfaces pos3/1

System Information::
    Links Count:         11
Link ID:: PO3/1 (10.0.0.33)
    Link Status:
      SRLGs:               1 2
      Physical Bandwidth:  2488000 kbits/sec
      Max Res Global BW:   20000 kbits/sec (reserved:0% in, 0% out)
      Max Res Sub BW:      5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   allow-all
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      IGP Neighbor:        ID 0000.0000.0004.00, IP 10.0.0.34 (Up)
      Flooding Status for each configured area [1]:
      IGP Area[1]: isis  level-2: flooded
```

Table 140 describes the significant fields shown in the displays.

Table 140 show mpls traffic-eng link-management interfaces Field Descriptions

Field	Description
Links Count	Number of links that were enabled for use with Multiprotocol Label Switching (MPLS) traffic engineering.
Link ID	Index of the link.
SRLGs	The SRLGs to which the link belongs.
Physical Bandwidth	Link's bandwidth capacity, in kBps.
Max Reservable BW	Amount of reservable bandwidth, in kb/s, on this link.
Max Res Global BW	Amount of reservable bandwidth, in kb/s, available for the global pool.
Max Res Sub BW	Amount of reservable bandwidth, in kb/s, available for the subpool.
MPLS TE Link State	The status of the MPLS link.
Inbound Admission	Link admission policy for inbound tunnels.
Outbound Admission	Link admission policy for outbound tunnels.
Admin. Weight	Administrative weight associated with this link.
IGP Neighbor Count	Number of Interior Gateway Protocol (IGP) neighbors directly reachable over this link.
IGP Neighbor	IGP neighbor on this link.
Flooding Status for each configured area	Flooding status for the specified configured area.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Displays local link information being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.
show mpls traffic-eng link-management igp-neighbors	Displays IGP neighbors.
show mpls traffic-eng link-management summary	Displays a summary of link management information.

show mpls traffic-eng link-management summary

To display a summary of link management information, use the **show mpls traffic-eng link-management summary** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng link-management summary [*interface-name*]

Syntax Description

interface-name	Specific interface for which information will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The output was enhanced to display Internet Gateway Protocol (IGP) recovery status provided by the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.

Examples

The following is sample output from the **show mpls traffic-eng link-management summary** command:

```
Router# show mpls traffic-eng link-management summary

System Information::
    Links Count:         2
    Flooding System:     enabled
IGP Area ID:: isis level-1
    Flooding Protocol:   ISIS
    Flooding Status:     data flooded
    Periodic Flooding:   enabled (every 180 seconds)
    Flooded Links:       1
    IGP System ID:       0001.0000.0001.00
    MPLS TE Router ID:   10.106.0.6
    IGP Neighbors:       1
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
Link ID:: AT0/0.2 (10.42.0.6)
    Link Status:
      Physical Bandwidth:  155520 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on
```

```
    Inbound Admission:   allow-all
    Outbound Admission:  allow-if-room
    Admin. Weight:       10 (IGP)
    IGP Neighbor Count:  0
```

Table 141 describes the significant fields shown in the display.

Table 141 show mpls traffic-eng link-management summary Field Descriptions

Field	Description
Links Count	Number of links configured for Multiprotocol Label Switching (MPLS) traffic engineering.
Flooding System	Enable status of the MPLS traffic engineering flooding system.
IGP Area ID	Name of the IGP area being described.
Flooding Protocol	IGP being used to flood information for this area.
Flooding Status	Status of flooding for this area.
Periodic Flooding	Status of periodic flooding for this area.
Flooded Links	Number of links that were flooded.
IGP System ID	IGP for this node associated with this area.
MPLS TE Router ID	MPLS traffic engineering router ID for this node.
IGP Neighbors	Number of reachable IGP neighbors associated with this area.
Link ID	Interface name and IP address of the link being described.
Physical Bandwidth	Link bandwidth capacity (in kBps).
Max Reservable BW	Amount of reservable bandwidth (in kBps) on this link.
MPLS TE Link State	Status of the link's MPLS traffic engineering-related functions.
Inbound Admission	Link admission policy for incoming tunnels.
Outbound Admission	Link admission policy for outgoing tunnels.
Admin. Weight	Link administrative weight.
IGP Neighbor Count	List of the IGP neighbors directly reachable over this link.

The following is sample output from the **show mpls traffic-eng link-management summary** command with the enhanced output, which shows the "IGP recovering" status, from the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature:

```
Router# show mpls traffic-eng link-management summary

System Information::
    Links Count:          3
    Flooding System:      enabled (IGP recovering)
IGP Area ID::  ospf  area nil
    Flooding Protocol:    OSPF
    Flooding Status:      data flooded
    Periodic Flooding:    enabled (every 180 seconds)
    Flooded Links:        0
```

Table 142 describes the significant fields shown in the display.

Table 142 show mpls traffic-eng link-management summary Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS traffic engineering.
Flooding System	Status of the MPLS traffic engineering flooding system. The notation (IGP recovering) indicates that status cannot be determined because an IP routing process restart is in progress.
IGP Area ID	Name of the IGP area being described.
Flooding Protocol	IGP being used to flood information for this area.
Flooding Status	Status of flooding for this area.
Periodic Flooding	Status of periodic flooding for this area.
Flooded Links	Number of links that were flooded.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.
show mpls traffic-eng link-management igp-neighbors	Displays IGP neighbors.
show mpls traffic-eng link-management interfaces	Displays per-interface resource and configuration information.

show mpls traffic-eng lsp attributes

To display global label switched path (LSP) attribute lists, use the **show mpls traffic-eng lsp attributes** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng lsp attributes [**name** *string*] [**internal**]

Syntax Description

name	(Optional) Identifies a specific LSP attribute list.
string	Describes the string argument.
internal	(Optional) Displays LSP atrribute list internal information.

Command Default

If no keywords or arguments are specified, all LSP attribute lists are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to display information about all LSP attribute lists or a specific LSP attribute list.

Examples

The following example shows output from the **show mpls traffic-eng lsp attributes** command:

```
Router# show mpls traffic-eng lsp attributes

LIST list1
    affinity 0xFF mask 0xFFFFFFFF
    auto-bw collect-bw
    bandwidth 12
    protection fast-reroute bw-protect
    lockdown
    priority 2 2
    record-route LIST 2
   bandwidth 5000
LIST hipriority
  priority 0 0
!
```

Table 143 describes the significant fields shown in the display.

Table 143 show mpls traffic-eng lsp attributes Field Descriptions

Field	Description
LIST	Identifies the LSP attribute list.
affinity	Indicates the LSP attribute that specifies attribute flags for LSP links. Values are 0 or 1.
mask	Indicates which attribute values should be checked.
auto-bw collect-bw	Indicates automatic bandwidth configuration.
protection fast re-route bw-protect	Indicates that the failure protection is enabled.
lockdown	Indicates that the reoptimization for the LSP is disabled.
priority	Indicates the LSP attribute that specifies LSP priority.
record-route	Indicates the record of the route used by the LSP.
bandwidth	Indicates the LSP attribute that specifies LSP bandwidth.

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.

show mpls traffic-eng process-restart iprouting

To display the status of IP routing and Multiprotocol Label Switching (MPLS) traffic engineering synchronization after an IP routing process restart, use the **show mpls traffic-eng process-restart iprouting** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng process-restart iprouting

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

This command displays information about the synchronization between the IP routing process and MPLS TE that you can provide to your technical support representative when you are reporting a problem.

All counters are set to zero when the system process initializes and are not reset no matter how often the IP routing process restarts.

The following is sample output from the **show mpls traffic-eng process-restart iprouting** command when an IP routing process has restarted normally:

```
Router# show mpls traffic-eng process-restart iprouting

IP Routing Restart Statistics:
  Current State: NORM
  Flushing State: IDLE

State Entered       Count     Timestamp            Timestamp            Timestamp
INIT                1         05/10/06-13:07:01
NORM                3         05/10/06-13:07:10    05/10/06-13:10:45   05/10/06-13:11:5
NORM-SPCT           0
AWAIT-CFG           2         05/10/06-13:10:32    05/10/06-13:11:45
CFG                 2         05/10/06-13:10:32    05/10/06-13:11:45
CMPL-FLSH           0
NCMPL-FLSH          2         05/10/06-13:10:32    05/10/06-13:11:45
NCMPL-FLSHD         2         05/10/06-13:10:32     05/10/06-13:11:45

Stuck State         Count     Timestamp             Timestamp          Timestamp
No Stuck states encountered

Counter             Count     Timestamp             Timestamp          Timestamp
Reg Succeed         40       05/10/06-13:11:51      05/10/06-13:11:45  05/10/06-13:11:45
Reg Fail             0
Incarnation          5       05/10/06-13:11:45      05/10/06-13:11:45  05/10/06-13:10:37
Flushing             2        05/10/06-13:10:32      05/10/06-13:11:45
```

Table 144 describes the normal output of the significant fields shown in the display. You should contact your technical support representative if your display has values other than those described in the table.

Table 144 show mpls traffic-eng process-restart iprouting Field Descriptions

Field	Description
Current State	This indicates the restart status. NORM indicates that routing convergence has occurred and that TE and the Internet Gateway Protocols (IGPs) have synchronized.
Flushing State	This indicates the flushing state. It should indicate IDLE.
Stuck State	This indicates the stuck state. The Count column should indicate that no stuck state has been encountered.
Reg Fail	This indicates a registry failure. The Count column should indicate 0.

Related Commands

Command	Description
debug mpls traffic-eng process-restart	Displays information about process restarts for reporting to your technical support representative.

show mpls traffic-eng topology

To display the Multiprotocol Label Switching (MPLS) traffic engineering global topology as currently known at the node, use the **show mpls traffic-eng topology** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng topology [**area** *area-id* | **level-1** | **level-2**] [*ip-address* [**brief** | **internal**] | **igp-id** {**isis** *nsapaddr* | **ospf** *ip-address* [**network** | **router**]} [**brief**] | **srlg**]

Syntax Description

area	(Optional) Restricts output to an Open Shortest Path First (OSPF) area.
area-id	The OSPF area ID. The range is from 0 to 4294967295.
level-1	(Optional) Restricts output to a System-to-Intermediate System (IS-IS) level-1.
level-2	(Optional) Restricts output to an IS-IS level-2.
ip-address	(Optional) The node by the IP address (router identifier to interface address).
brief	(Optional) Provides a less detailed version of the topology.
internal	(Optional) Specifies to use the internal format.
igp-id	(Optional) Specifies the node by Interior Gateway Protocol (IGP) router identifier.
isis *nsapaddr*	Specifies the node by router identification if using Intermediate IS-IS.
ospf *ip-address*	Specifies the node by router identifier if using OSPF.
network	(Optional) Specifies the node type as network.
router	(Optional) Specifies the node type as router.
srlg	(Optional) Displays Shared Risk Link Groups (SRLG) membership for each link in a topology.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(11)ST	This command was modified. The single “Reservable” column was replaced by two columns: one each for “global pool” and for “subpool.”
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(28)SB	This command was modified. The **area**, **level-1**, and **level-2** keywords were added.

Release	Modification
12.2(33)SRA	This command was modified and integrated into Cisco IOS Release 12.2(33)SRA. The **srlg** keyword was added.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows output from the **show mpls traffic-eng topology** command:

```
Router# show mpls traffic-eng topology

My_System_id: 0000.0000.0001.00 (isis 1 level-2)
My_System_id: 10.10.10.10 (ospf 100 area 0)
My_BC_Model_Type: MAM

Signalling error holddown: 10 sec Global Link Generation 56

IGP Id: 0000.0000.0001.00, MPLS TE Id: 10.10.10.10 Router Node  (isis 1 level-2)

  Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0002.00, Nbr Node Id:6, gen:56
      Frag Id:0, Intf Address:10.2.2.1, Intf Id:0
       Nbr Intf Address:10.2.2.2, Nbr Intf Id:0
      TE Metric:10, IGP Metric:10, Attribute Flags:0x0
      Switching Capability:, Encoding:
      BC Model ID:MAM
      Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps)
      BC0:600 (kbps) BC1:400 (kbps)
                     Total Allocated   Reservable
                     BW (kbps)         BW (kbps)
                     ---------------   -----------
        TE-class[0]:            0            600
        TE-class[1]:            0            400
        TE-class[2]:            0              0
        TE-class[3]:            0              0
        TE-class[4]:            0            600
        TE-class[5]:            0            400
        TE-class[6]:            0              0
        TE-class[7]:            0              0

  Link[1]:Point-to-Point, Nbr IGP Id:0000.0000.0002.00, Nbr Node Id:6, gen:56
      Frag Id:0, Intf Address:10.1.1.1, Intf Id:0
       Nbr Intf Address:10.1.1.2, Nbr Intf Id:0
      TE Metric:10, IGP Metric:10, Attribute Flags:0x0
      Switching Capability:, Encoding:
      BC Model ID:MAM
      Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps)
      BC0:600 (kbps) BC1:400 (kbps)
                     Total Allocated   Reservable
                     BW (kbps)         BW (kbps)
                     ---------------   -----------
        TE-class[0]:           10            590
        TE-class[1]:            0            400
        TE-class[2]:            0              0
        TE-class[3]:            0              0
        TE-class[4]:            0            600
        TE-class[5]:            0            400
        TE-class[6]:            0              0
        TE-class[7]:            0              0
```

Table 145 describes significant fields shown in the display.

Table 145 show mpls traffic-eng topology Field Descriptions

Field	Description
My_System_id	Unique identifier of the IGP.
My_BC_Model_Type: MAM	Bandwidth constraints model of the local node: either Maximum Allocation Model (MAM) or Russian Dolls Model (RDM).
Signalling error holddown:	Link hold-down timer configured to handle path error events to exclude link from topology.
IGP Id	Identification of the advertising router.
MPLS TE Id	Unique MPLS traffic engineering node identifier.
Intf Id:	Interface identifier.
Router Node	Type of node.
Nbr IGP Id	Neighbor IGP router identifier.
Intf Address	The interface address of the link.
Nbr Intf Address:	IP address of the neighbor interface.
BC Model ID:	Bandwidth Constraints Model ID: RDM or MAM.
gen	Generation number of the link-state packet (LSP). This internal number is incremented when any new LSP is received.
Frag Id	IGP link-state advertisement (LSA) fragment identifier.
TE Metric	TE cost of the link.
IGP Metric	IGP cost of the link.
Attribute Flags	The requirements on the attributes of the links that the traffic crosses.
Physical BW	Physical line rate.
Max Reservable BW	Maximum amount of bandwidth, in kilobits per second (kb/s), that can be reserved on a link.
Total Allocated	Amount of bandwidth, in kb/s, allocated at that priority.
Reservable	Amount of available bandwidth, in kb/s, reservable for that TE-Class for two pools: BC0 (formerly called “global”) and BC1 (formerly called “sub”).

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays information about tunnels.

show mpls traffic-eng topology path

To show the properties of the best available path to a specified destination that satisfies certain constraints, use the **show mpls traffic-eng topology path** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng topology path {*tunnel-interface* [**destination** *address*] | **destination** *address*} [**bandwidth** *value*] [**priority** *value* [*value*]] [**affinity** *value* [**mask** *mask*]]

Syntax Description

tunnel-interface	Name of an MPLS traffic engineering interface (for example, Tunnel1) from which default constraints should be copied.
destination *address*	(Optional) IP address specifying the path's destination.
bandwidth *value*	(Optional) Bandwidth constraint. The amount of available bandwidth that a suitable path requires. This overrides the bandwidth constraint obtained from the specified tunnel interface. You can specify any positive number.
priority *value* [*value*]	(Optional) Priority constraints. The setup and hold priorities used to acquire bandwidth along the path. If specified, this overrides the priority constraints obtained from the tunnel interface. Valid values are from 0 to 7.
affinity *value*	(Optional) Affinity constraints. The link attributes for which the path has an affinity. If specified, this overrides the affinity constraints obtained from the tunnel interface.
mask *mask*	(Optional) Affinity constraints. The mask associated with the affinity specification.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The specified constraints override any constraints obtained from a reference tunnel.

Examples

The following is sample output from the **show mpls traffic-eng topology path** command:

```
Router # show mpls traffic-eng topology path Tunnel1 bandwidth 1000

Query Parameters:
  Destination:10.112.0.12
    Bandwidth:1000
   Priorities:1 (setup), 1 (hold)
     Affinity:0x0 (value), 0xFFFF (mask)
Query Results:
  Min Bandwidth Along Path:2000 (kbps)
  Max Bandwidth Along Path:5000 (kbps)
  Hop  0:10.1.0.6       :affinity 00000000, bandwidth 2000 (kbps)
  Hop  1:10.1.0.10      :affinity 00000000, bandwidth 5000 (kbps)
  Hop  2:10.43.0.10     :affinity 00000000, bandwidth 2000 (kbps)
  Hop  3:10.112.0.12
```

Table 146 describes the significant fields shown in the display.

Table 146 show mpls traffic-eng topology path Field Descriptions

Field	Description
Destination	IP address of the path's destination.
Bandwidth	Amount of available bandwidth that a suitable path requires.
Priorities	Setup and hold priorities used to acquire bandwidth.
Affinity	Link attributes for which the path has an affinity.
Min Bandwidth Along Path	Minimum amount of bandwidth configured for a path.
Max Bandwidth Along Path	Maximum amount of bandwidth configured for a path.
Hop	Information about each link in the path.

show mpls traffic-eng tunnels

To display information about tunnels, use the **show mpls traffic-eng tunnels** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng tunnels [[**attributes** *list-name*] [**destination** *address*] [**down**] [**interface** *type number*] [**name** *name*] [**name-regexp** *reg-exp*] [**property** {**auto-tunnel** {**backup** | **mesh** | **primary**} | **backup-tunnel** | **fast-reroute**}] [**role** {**all** | **head** | **middle** | **remote** | **tail**}] [**source-id** {*ipaddress* [*tunnel-id*]}] [**suboptimal constraints** {**current** | **max** | **none**}] [**up**]] [**accounting** | **brief** | **protection**]

Syntax Description

attributes *list-name*	(Optional) Restricts the display to tunnels that use a matching attributes list.
destination *address*	(Optional) Restricts the display to tunnels destined to the specified IP address.
down	(Optional) Displays tunnels that are not active.
interface	(Optional) Displays information for the specified interface.
type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
name *name*	(Optional) Displays the tunnel with the specified string. The tunnel string is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel string is included in the signaling message so that it is available at all hops.
name-regexp *regexp*	(Optional) Displays tunnels whose descriptions match the specified regular expression.
property	(Optional) Displays tunnels with the specified property.
auto-tunnel	Displays information about autotunnels.
backup	Displays information about the Fast Reroute protection provided by each tunnel selected by other options specified with this command. The information includes the physical interface protected by the tunnel, the number of traffic engineering (TE) label switched packets (LSPs) (that is, tunnels) protected, and the bandwidth protected.
mesh	Displays information about auto-tunnel mesh tunnel interfaces.
primary	Displays information about auto-tunnel primary tunnel interfaces.
backup-tunnel	Displays information about the Fast Reroute protection provided by each tunnel selected by other options specified with this command. The information includes the physical interface protected by the tunnel, the number of traffic engineering (TE) label switched packets (LSPs) (that is, tunnels) protected, and the bandwidth protected.
fast-reroute	Selects Fast Reroute-protected MPLS TE tunnels originating, transmitting, or terminating on this router.
role	Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
all	Displays all tunnels.

head	Displays tunnels with their head at this router.
middle	Displays tunnels with a midpoint at this router.
remote	Displays tunnels with their head at some other router; this is a combination of **middle** and **tail**.
tail	Displays tunnels with a tail at this router.
source-id	(Optional) Restricts the display to tunnels with a matching source IP address or tunnel number.
ipaddress	Source IP address.
tunnel-id	Tunnel number. The range is from 0 to 65535.
suboptimal	(Optional) Displays information about tunnels using a suboptimal path.
constraints	Specifies constraints for finding the best comparison path.
current	Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options. Selected tunnels would have a shorter path if they were reoptimized immediately.
max	Displays information for the specified tunneling interface.
none	Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the Interior Gateway Protocol's (IGP) shortest path.
up	(Optional) Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
accounting	(Optional) Displays accounting information (the rate of the traffic flow) for tunnels.
brief	(Optional) Specifies a format with one line per tunnel.
protection	(Optional) Displays information about the protection provided by each tunnel selected by other options specified with this command. The information includes whether protection is configured for the tunnel, the protection (if any) provided to the tunnel by this router, and the bandwidth protected.

Command Default

General information about each MPLS TE tunnel known to the router is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	Input and output interface information was added to the new **brief** form of the output. The **suboptimal** and **interface** keywords were added to the nonbrief format. The nonbrief, nonsummary formats contain the history of the LSP selection.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	The **property** and **protection** keywords were added. The command is supported on the Cisco 10000 series routers.

Release	Modification
12.2(18)S	The following keywords were added: **accounting**, **attributes**, **name-regexp**, and **property auto-tunnel**. The **property backup** keyword was changed to **property backup-tunnel**.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The **detail** and **dest-mode** keywords were added. The output was updated to display MPLS TE P2MP information. The command output was enhanced to include the configuration and status when a path option list is configured for backup path options. The output also shows information about tunnels configured with autoroute announce.

Usage Guidelines

To select the tunnels for which information is displayed, use the **auto-tunnel**, **backup-tunnel**, **attributes**, **destination**, **interface**, **name**, **name-regexp**, **property**, **role**, **source-id**, **suboptimal constraints, up**, and **down** keywords singly or combined.

To select the type of information displayed about the selected tunnels, use the **accounting**, **backup**, **protection**, **statistics**, and **summary** keywords.

The **auto-tunnel**, **backup-tunnel**, and **property** keywords display the same information, except that the **property** keyword restricts the display to autotunnels, backup tunnels, or tunnels that are Fast Reroute-protected.

The **name-regexp** keyword displays output for each tunnel whose name contains a specified string. For example, if there are tunnels named iou-100-t1, iou-100-t2, and iou-100-t100, the **show mpls traffic-eng tunnels name-regexp iou-100** command displays output for the three tunnels whose name contains the string iou-100.

If you specify the **name** keyword, there is command output only if the command name is an exact match; for example, iou-100-t1.

The nonbrief and nonsummary formats of the output contain the history of the LSP selection.

The "Reroute Pending" State Changes in Cisco IOS Release 12.2(33)SRE

In releases before Cisco IOS Release 12.2(33)SRE, MPLS TE P2P tunnels display "reroute pending" during reoptimization until the "delayed clean" status of the old path is complete. During the "delayed clean" process, the command output displays the following status:

```
Router# show mpls traffic-eng tunnels tunnel 534

Name: Router_t534                         (Tunnel534) Destination: 10.30.30.8
    Status:
      Admin: up         Oper: up     Path: valid       Signalling: connected
      path option 10, type explicit PRIMARY_TO_8 (Basis for Setup, path weight 30)
  !!! path option 10 delayed clean in progress
  !!!     Change in required resources detected: reroute pending
          Currently Signalled Parameters:
            Bandwidth: 300      kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
            Metric Type: TE (default)
```

In Cisco IOS Release 12.2(33)SRE and later releases, P2P and P2MP MPLS TE tunnels display “reroute pending” during reoptimization until the new path is used for forwarding. The “reroute pending” status is not displayed during the delayed clean operation. There is no change to data forwarding or tunnel creation. You might see the “reroute pending” status for a shorter time. In the following example, the “reroute pending” message appears, but the “delayed clean” message does not.

```
Router# show mpls traffic-eng tunnels tunnel 534

  Name: Router_t534                         (Tunnel534) Destination: 10.30.30.8
    Status:
      Admin: up         Oper: up     Path: valid       Signalling: connected
      path option 10, type explicit PRIMARY_TO_8 (Basis for Setup, path weight 30)
            Change in required resources detected: reroute pending
          Currently Signalled Parameters:
            Bandwidth: 300      kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
            Metric Type: TE (default)
```

Examples

The following is sample output from the **show mpls traffic-eng tunnels brief** command. It displays brief information about every MPLS TE tunnel known to the router.

```
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 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         PO4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Table 120 describes the significant fields shown in the display.

Table 147 show mpls traffic-eng tunnels Field Descriptions

Field	Description
LSP Tunnels Process	Status of the LSP tunnels process.
RSVP Process	Status of the Resource Reservation Protocol (RSVP) process.
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Schedule for periodic reoptimization (in seconds).
TUNNEL NAME	Name of the interface that is configured at the tunnel head.
DESTINATION	Identifier of the tailend router.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.
STATE/PROT	For tunnel heads, the value is admin-down, up, or down. For nonheads, the value is signaled.

MPLS Traffic Engineering Fast Reroute Examples

The following is sample output from the **show mpls traffic-eng tunnels property fast-reroute brief** command. It displays brief information about all MPLS TE tunnels acting as Fast Reroute backup tunnels (**property backup-tunnel**) for interfaces on the router.

```
Router# show mpls traffic-eng tunnels property fast-reroute brief

Signalling Summary:
    LSP Tunnels Process:            running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 2231 seconds
    Periodic FRR Promotion:         every 300 seconds, next in 131 seconds
    Periodic auto-bw collection:    disabled
TUNNEL NAME                     DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t2000                    10.110.0.10      -         PO4/0/1   up/up
Router_t2                       10.112.0.12      -         unknown   up/down
Router_t3                       10.112.0.12      -         unknown   admin-down
Displayed 3 (of 9) heads, 0 (of 1) midpoints, 0 (of 0) tails
```

The following is sample output from the **show mpls traffic-eng tunnels backup** command. This command selects every MPLS TE tunnel known to the router and displays information about the Fast Reroute protection each selected tunnels provides for interfaces on this router; the command does not generate output for tunnels that do not provide Fast Reroute protection of interfaces on this router.

```
Router# show mpls traffic-eng tunnels backup

Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 192.168.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

The following is sample output from the **show mpls traffic-eng tunnels property fast-reroute protection** command. This command selects every MPLS TE tunnel known to the router that was signaled as a Fast Reroute-protected LSP (**property fast-reroute**) and displays information about the protection this router provides each selected tunnel.

```
Router# show mpls traffic-eng tunnels property fast-reroute protection

Router_t1
  LSP Head, Tunnel1, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 25
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
```

```
      Backup Tu5711 to LSP nhop
        Tu5711: out i/f: PO1/1, label: implicit-null
      LSP signalling info:
        Original: out i/f: PO1/0, label: 12304, nhop: 10.1.1.7
        With FRR: out i/f: Tu5711, label: 12304
      LSP bw: 6000 kbps, Backup level: any unlimited, type: any pool
Router_t2
  LSP Head, Tunnel2, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 2
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
      Backup Tu578 to LSP nhop
        Tu578: out i/f: PO1/0, label: 12306
      LSP signalling info:
        Original: out i/f: PO3/3, label: implicit-null, nhop: 10.3.3.8
        With FRR: out i/f: Tu578, label: implicit-null
      LSP bw: 100 kbps, Backup level: any unlimited, type: any pool
r9_t1
  LSP Midpoint, signalled, connection up
  Src 10.9.9.9, Dest 10.88.88.88, Instance 2347
  Fast Reroute Protection: Requested
    Inbound:  FRR Inactive
      LSP signalling info:
        Original: in i/f: PO1/2, label: 12304, phop: 10.205.0.9
    Outbound: FRR Ready
      Backup Tu5711 to LSP nhop
        Tu5711: out i/f: PO1/1, label: implicit-null
      LSP signalling info:
        Original: out i/f: PO1/0, label: 12305, nhop: 10.1.1.7
        With FRR: out i/f: Tu5711, label: 12305
      LSP bw: 10 kbps, Backup level: any unlimited, type: any pool
```

The following is sample output from the **show mpls traffic-eng tunnels tunnel** command. This command displays information about just a single tunnel.

```
Router# show mpls traffic-eng tunnels tunnel 1

Name: swat76k1_t1                          (Tunnel1) Destination: 10.0.0.4
   Status:
     Admin: admin-down Oper: down   Path: not valid   Signalling: Down
     path option 1, type explicit gi7/4-R4

   Config Parameters:
     Bandwidth: 0        kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
     Metric Type: TE (default)
     AutoRoute:  disabled  LockDown: disabled  Loadshare: 0        bw-based
     auto-bw: disabled

   Shortest Unconstrained Path Info:
     Path Weight: 2 (TE)
     Explicit Route: 10.1.0.1 10.1.0.2 172.0.0.1 192.0.0.4
   History:
     Tunnel:
       Time since created: 13 days, 52 minutes
       Number of LSP IDs (Tun_Instances) used: 0 swat76k1#
swat76k1#sh mpls traf tun property ?
   auto-tunnel    auto-tunnel created tunnels
   backup-tunnel  Tunnels used as fast reroute
   fast-reroute   Tunnels protected by fast reroute
```

The following is sample output from the **show mpls traffic-eng tunnels accounting** command. This command displays the rate of the traffic flow for the tunnels.

```
Router# show mpls traffic-eng tunnels accounting

Tunnel1 (Destination 10.103.103.103; Name iou-100_t1)
 5 minute output rate 0 kbits/sec, 0 packets/sec
Tunnel2 (Destination 10.103.103.103; Name iou-100_t2)
 5 minute output rate 0 kbits/sec, 0 packets/sec Tunnel100 (Destination 10.101.101.101;
Name iou-100_t100)
 5 minute output rate 0 kbits/sec, 0 packets/sec Totals for 3 Tunnels
 5 minute output rate 0 kbits/sec, 0 packets/sec
```

MPLS Traffic Engineering Point-to-Multipoint Command Examples

When the MPLS TE P2MP feature is configured, the **show mpls traffic-eng tunnels** command categorizes the output as follows:

- P2P tunnels/LSPs
- P2MP tunnels
- P2MP sub-LSPs

The following **show mpls traffic-eng tunnels brief** command displays P2MP tunnel and sub-LSP information:

```
Router# show mpls traffic-eng tunnels brief

Signalling Summary:
   LSP Tunnels Process:            running
   Passive LSP Listener:           running
   RSVP Process:                   running
   Forwarding:                     enabled
   Periodic reoptimization:        every 60 seconds, next in 5 seconds
   Periodic FRR Promotion:         Not Running
   Periodic auto-bw collection:    disabled

P2P TUNNELS/LSPs:
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
p2p-LSP                          10.2.0.1         -         Se2/0     up/up
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails

P2MP TUNNELS:
                        DEST    CURRENT
INTERFACE   STATE/PROT UP/CFG TUNID LSPID
Tunnel2     up/up      3/10   2     1
Tunnel5     up/down    1/10   5     2
Displayed 2 (of 2) P2MP heads

P2MP SUB-LSPS:
SOURCE          TUNID LSPID   DESTINATION     SUBID     ST UP IF    DOWN IF
10.1.0.1        2     1       10.2.0.1        1         up head     Se2/0
10.1.0.1        2     1       10.3.0.199      2         up head     Et2/0
10.1.0.1        2     1       19.4.0.1        2         up head     s2/0
10.1.0.1        2     2       1 9.4.0.1       2         up head     s2/0
10.1.0.1        5     2       10.5.0.1        7         up head     e2/0
100.100.100.100 1     3       200.200.200.200 1         up ge2/0    s2/0
100.100.100.100 1     3       10.1.0.1        1         up e2/0     tail
Displayed 7 P2MP sub-LSPs:
          5 (of 5) heads, 1 (of 1) midpoints, 1 (of 1) tails
```

The following **show mpls traffic-eng tunnels statistics** command displays status information about P2MP path and LSPs for Tunnel 100:

```
Router# show mpls traffic-eng tunnels statistics
```

```
Tunnel100 (Name p2mp-1_t100)
  Management statistics:
    Path:   0 no path, 0 path no longer valid, 0 missing ip exp path
            97 path changes, 306 path lookups
            0 protection pathoption_list errors
            0 invalid inuse popt in pathoption list
            0 loose path reoptimizations, triggered by PathErrors
    State:  1 transitions, 0 admin down, 0 oper down
  Signalling statistics:
    Opens:  1 succeeded, 0 timed out, 0 bad path spec
            0 other aborts
      LSP Activations: 97 succeeded
        Last Failure: No path that satisfy tunnel constraints
        Failures stats:
          5: No path that satisfy tunnel constraints
    Errors: 0 no b/w, 288 no route, 0 admin, 0 remerge detected
            0 bad exp route, 0 rec route loop, 0 frr activated
            0 other
```

The following **show mpls traffic-eng tunnels summary** command displays information about P2MP LSPs and sub-LSPs:

```
Router# show mpls traffic-eng tunnels statistics

Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 2599 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    disabled
    P2P:
      Head: 10 interfaces,   0 active signalling attempts, 0 established
            0 activations,  0 deactivations
            0 SSO recovery attempts, 0 SSO recovered
      Midpoints: 0, Tails: 1

    P2MP:
      Head: 6 interfaces,   3 active signalling attempts, 3 established
            291 sub-LSP activations,  288 sub-LSP deactivations
            97 LSP successful activations,  96 LSP deactivations
            5 LSP failed activations
            SSO: Unsupported
      Midpoints: 0, Tails: 0
```

The following is sample output from the **show mpls traffic-eng tunnels** command for a tunnel named t1. The output includes an adjustment threshold of 5 percent, an overflow limit of 4, an overflow threshold of 25 percent, and an overflow threshold exceeded of 1.

```
Router# show mpls traffic-eng tunnels name t1

Name:tagsw4500-9_t1 (Tunnel1) Destination:10.0.0.4
 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:13 kbps (Global) Priority:7 7 Affinity:0x0/0xFFFF
 AutoRoute: disabled LockDown:disabled Loadshare:13 bw-based
 auto-bw:(300/265) 53 Bandwidth Requested: 13
   Adjustment threshold: 5%
```

```
   Overflow Limit: 4  Overflow Threshold: 25%
  Overflow Threshold Crossed: 1
  Sample Missed: 1 Samples Collected: 1
Active Path Option Parameters:
  State: dynamic path option 1 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
 InLabel  :  -
 OutLabel : Serial3/0, 18
 RSVP Signalling Info:
   Src 10.0.0.1, Dst 10.0.0.4, Tun_Id 2, Tun_Instance 2
  RSVP Path Info:
   My Address: 10.105.0.1
   Explicit Route: 10.105.0.2 104.105.0.1 10.0.0.4
   Record   Route:   NONE
   Tspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
 Record   Route:   NONE
   Tspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
  RSVP Resv Info:
   Record   Route:   NONE
   Fspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
  Shortest Unconstrained Path Info:
   Path Weight: 128 (TE)
   Explicit Route: 10.105.0.2 104.105.0.1 10.0.0.4
  History:
   Tunnel:
    Time since created: 7 minutes, 56 seconds
     Time since path change: 7 minutes, 18 seconds
     Number of LSP IDs (Tun_Instances) used: 2
     Number of Auto-bw Adjustment resize requests: 1
     Time since last Auto-bw Adjustment resize request: 1 minutes, 7 seconds
     Number of Auto-bw Overflow resize requests: 1
     Time since last Auto-bw Overflow resize request: 52 seconds
     Current LSP:
      Uptime: 52 seconds
      Selection: reoptimization
    Prior LSP:
ID: path option 1 [1]
  Removal Trigger: configuration changed
```

The following sample output from the **show mpls traffic-eng tunnels tunnel** command for Cisco IOS Release 12.2(33)SRE shows path protection information. This command displays information about a single tunnel.

```
Router# show mpls traffic-eng tunnels tunnel 1

Name: iou-100_t2 (Tunnel2) Destination: 10.10.0.2
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit primary1 (Basis for Setup, path weight 10)
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type list name secondary-list
   Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)

Config Parameters:
 Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
 Metric Type: TE (default)
 AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
 auto-bw: disabled
Active Path Option Parameters:
 State: explicit path option 10 is active
 BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet7/0, implicit-null
```

```
RSVP Signalling Info:
 Src 100.100.100.100, Dst 10.10.0.2, Tun_Id 2, Tun_Instance 188
RSVP Path Info:
 My Address: 10.1.0.1
 Explicit Route: 10.1.0.2 10.10.0.2
 Record Route: NONE
 Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
 Record Route: NONE
 Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
 Path Weight: 10 (TE)
 Explicit Route: 10.1.0.1 10.1.0.2 10.10.0.2
History:
 Tunnel:
  Time since created: 1 hours, 34 minutes
  Time since path change: 1 minutes, 50 seconds
  Number of LSP IDs (Tun_Instances) used: 188
 Current LSP:
  Uptime: 1 minutes, 50 seconds
 Prior LSP:
  ID: path option 10 [44]
  Removal Trigger: label reservation removed
```

The following sample output from the **show mpls traffic-eng tunnels** command for Cisco IOS Release 12.2(33)SRE shows autoroute destination information.

```
Router# show mpls traffic-eng tunnel tunnel 109

Name: PE-7_t109                    (Tunnel109) Destination: 10.0.0.9
 Status:
  Admin: up   Oper: up   Path: valid Signalling: connected
  path option 1, type explicit to_109 (Basis for Setup, path weight 64)
  path option 20, type explicit to_109_alt

Config Parameters:
 Bandwidth: 0   kbps (Global   Priority: 7  7   Affinity: 0x0/0xFFFF
 Metric Type: TE (default)
 Autoroute announce: enabled LockDown: disabled   Loadshare: 0    bx-based
 auto-bw: disabled
 AutoRoute destination: enabled
```

Table 148 describes the significant fields shown in the display.

Table 148 show mpls traffic-eng tunnels Field Descriptions

Field	Description
LSP Tunnels Process	Status of the LSP tunnels process.
RSVP Process	Status of the Resource Reservation Protocol (RSVP) process.
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Schedule for periodic reoptimization (in seconds).
TUNNEL NAME	Name of the interface that is configured at the tunnel head.
DESTINATION	Identifier of the tailend router.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.

Table 148 show mpls traffic-eng tunnels Field Descriptions (continued)

Field	Description
STATE/PROT	For tunnel heads, admin-down, up, or down. For nonheads, signaled.
Adjustment threshold	Configured threshold. This field is displayed only if a threshold is explicitly configured.
Overflow Limit Overflow Threshold	Resized the tunnel before the end of the sampling interval if the output rate exceeded the current bandwidth by the percent specified in the overflow threshold the number of times specified in the overflow limit. These fields are displayed only if an overflow limit was specified in the **tunnel mpls traffic-eng auto-bw** command.
Overflow Threshold Crossed	Number of times the output rate exceeded the overflow threshold in consecutive collection intervals. This value is reset at the beginning of the automatic bandwidth sampling interval.
Number of Auto-bw Adjustment resize requests	Number of times the tunnel was resized because an output rate exceeded the adjustment threshold. This field is displayed only if the number is greater than zero and if automatic bandwidth is enabled on the tunnel. This counter is reset each time automatic bandwidth is enabled on the tunnel. You can clear this counter at any time by entering the **clear mpls traffic-eng auto-bw timer** command.
Time since last Auto-bw Adjustment resize request	The amount of time (in minutes and seconds) since the last bandwidth adjustment.
Number of Auto-bw Overflow resize requests	The number of times (in seconds) the tunnel was resized because an overflow limit was exceeded. This field is displayed only if the number is greater than zero and if an overflow limit is enabled on the tunnel. This counter is reset each time automatic bandwidth is enabled on the tunnel. You can clear this counter at any time by entering the **clear mpls traffic-eng auto-bw timer** command.
Time since last Auto-bw Overflow resize request	The amount of time (in seconds) since the tunnel was resized because an overflow limit was exceeded.

Related Commands

Command	Description
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng tunnels (configuration)	Enables MPLS traffic engineering tunnel signaling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signaling on an interface.

sshow mpls traffic-eng tunnels statistics

To display event counters for one or more Multiprotocol Label Switching (MPLS) traffic engineering tunnels, use the **show mpls traffic-eng tunnels statistics** command in user EXEC and privileged EXEC mode.

show mpls traffic-eng tunnels [**tunnel** *tunnel-name*] **statistics** [**summary**]

Syntax Description

tunnel *tunnel-name*	(Optional) Displays event counters accumulated for the specified tunnel.
summary	(Optional) Displays event counters accumulated for all tunnels.

Defaults

If you enter the command without any keywords, the command displays the event counters for every MPLS traffic engineering tunnel interface configured on the router.

Command Modes

User EXEC (>)
Privileged EXEC mode (#)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

A label switching router (LSR) maintains counters for each MPLS traffic engineering tunnel headend that counts significant events for the tunnel, such as state transitions for the tunnel, changes to the tunnel path, and various signaling failures. You can use the **show mpls traffic-eng tunnels statistics** command to display these counters for a single tunnel, for every tunnel, or for all tunnels (accumulated values). Displaying the counters is often useful for troubleshooting tunnel problems.

Examples

The following are examples of output from the **show mpls traffic-eng tunnels statistics** command:

```
Router# show mpls traffic-eng tunnels tunnel tunnel1001 statistics

Tunnel1001 (Destination 10.8.8.8; Name Router_t1001)
  Management statistics:
    Path:25 no path, 1 path no longer valid, 0 missing ip exp path
    5 path changes
    State:3 transitions, 0 admin down, 1 oper down
```

```
  Signalling statistics:
    Opens:2 succeeded, 0 timed out, 0 bad path spec
    0 other aborts
    Errors:0 no b/w, 0 no route, 0 admin
    0 bad exp route, 0 rec route loop, 0 other


Router# show mpls traffic-eng tunnels statistics

Tunnel1001 (Destination 10.8.8.8; Name Router_t1001)
  Management statistics:
    Path:25 no path, 1 path no longer valid, 0 missing ip exp path
    5 path changes
    State:3 transitions, 0 admin down, 1 oper down
  Signalling statistics:
    Opens:2 succeeded, 0 timed out, 0 bad path spec
    0 other aborts
    Errors:0 no b/w, 0 no route, 0 admin
    0 bad exp route, 0 rec route loop, 0 other
.
.
.
Tunnel7050 (Destination 10.8.8.8; Name Router_t7050)
  Management statistics:
    Path: 19 no path, 1 path no longer valid, 0 missing ip exp path
    3 path changes
    State: 3 transitions, 0 admin down, 1 oper down
  Signalling statistics:
    Opens: 2 succeeded, 0 timed out, 0 bad path spec
    0 other aborts
    Errors:0 no b/w, 0 no route, 0 admin
    0 bad exp route, 0 rec route loop, 0 other


Router# show mpls traffic-eng tunnels statistics summary

  Management statistics:
    Path:2304 no path, 73 path no longer valid, 0 missing ip exp path
    432 path changes
    State:300 transitions, 0 admin down, 100 oper down
  Signalling statistics:
    Opens:200 succeeded, 0 timed out, 0 bad path spec
    0 other aborts
    Errors:0 no b/w, 18 no route, 0 admin
    0 bad exp route, 0 rec route loop, 0 other
```

Table 149 describes the significant fields shown in the display.

Table 149 show mpls traffic-eng tunnels statistics Field Descriptions

Field	Description
Tunnel 1001	Name of the tunnel interface.
Destination	IP address of the tunnel tailend.
Name	Internal name for the tunnel, composed of the router name and the tunnel interface number.

Table 149 show mpls traffic-eng tunnels statistics Field Descriptions (continued)

Field	Description
Path	Heading for counters for tunnel path events are as follows: • no path—Number of unsuccessful attempts to calculate a path for the tunnel. • path no longer valid—Number of times a previously valid path for the tunnel became invalid. • missing ip exp path—Number of times that attempts to use "obtain a path for the tunnel" failed because no path was configured (and there was no dynamic path option for the tunnel). • path changes—Number of times the tunnel path changed.
State	Heading for counters for tunnel state transitions.
Opens	Heading for counters for tunnel open attempt events.
Errors	Heading for various tunnel signaling errors, such as no bandwidth, no route, admin (preemption), a bad explicit route, and a loop in the explicit route.

Related Commands

Command	Description
clear mpls traffic-eng tunnel counters	Clears the counters for all MPLS traffic engineering tunnels.

show mpls traffic-eng tunnels summary

To display summary information about tunnels, use the **show mpls traffic-eng tunnels summary** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng tunnels summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	The command output was updated to display periodic Fast Reroute information. The command is supported on the Cisco 10000 series ESRs.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	The command output was modified to display the number of tunnels that were attempted and successful in being recovered following a failover.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show mpls traffic-eng tunnels summary** command to display the number of tunnel headends that were attempted and successful at being recovered following a stateful switchover (SSO).

Examples

The following is sample output from the **show mpls traffic-eng tunnels summary** command**:**

```
Router# show mpls traffic-eng tunnels summary

Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    Head: 3 interfaces, 3 active signalling attempts, 3 established
          3 activations, 3 deactivations
          3 SSO recovery attempts, 3 SSO recovered
    Midpoints: 1, Tails: 0
    Periodic reoptimization:        every 3600 seconds, next in 873 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 273 seconds
```

Table 150 describes the significant fields shown in the display.

Table 150 show mpls traffic-eng tunnels summary Field Descriptions

Field	Description
LSP Tunnels Process	Multiprotocol Label Switching (MPLS) traffic engineering has or has not been enabled.
Passive LSP Listener	The device listens for LSPs and can terminate them, if desired.
RSVP Process	Resource Reservation Protocol (RSVP) has or has not been enabled. (This feature is enabled as a consequence of MPLS traffic engineering being enabled.)
Forwarding	Indicates whether appropriate forwarding is enabled. (Appropriate forwarding on a router is Cisco Express Forwarding switching.)
Head	Summary information about tunnel heads at this device. Information includes: • interfaces—Number of MPLS traffic engineering tunnel interfaces. • active signalling attempts—Number of LSPs currently successfully signaled or being signaled. • established—Number of LSPs currently signaled. • activations—Number of signaling attempts initiated. • deactivations—Number of signaling attempts terminated. • SSO recovery attempts—Number of MPLS traffic engineering tunnel headend LSPs that were attempted to be recovered following an SSO event. • SSO recovered—Number of MPLS traffic engineering tunnel headend LSPs that were successfully recovered following an SSO event.
Midpoints	Number of midpoints at this device.
Tails	Number of tails at this device.
Periodic reoptimization	Frequency of periodic reoptimization and time (in seconds) until the next periodic reoptimization.
Periodic FRR Promotion	Frequency that scanning occurs to determine if link-state packets (LSPs) should be promoted to better backup tunnels, and time (in seconds) until the next scanning.
Periodic auto-bw collection	Frequency of automatic bandwidth collection and time left (in seconds) until the next collection.

Related Commands

Command	Description
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng tunnels (configuration)	Enables MPLS traffic engineering tunnel signaling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signaling on an interface.

show mpls ttfib

To display information about the Multiprotocol Label Switching (MPLS) TTFIB table, use the **show mpls ttfib** command in EXEC mode.

show mpls ttfib [**detail** [**hardware**] | **vrf** *instance* [**detail**]]

Syntax Description

detail	(Optional) Displays detailed information.
hardware	(Optional) Displays detailed hardware information.
vrf *instance*	(Optional) Displays entries for a specified Virtual Private Network (VPN) routing and forwarding instance (VRF).

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display information about the MPLS TTFIB table:

```
Router# show mpls ttfib

Local  Outgoing    Packets Tag          LTL   Dest.   Destination    Outgoing
Tag    Tag or VC   Switched             Index Vlanid  Mac Address    Interface
4116   21          0                    0xE0  1020    0000.0400.0000 PO4/1*
       34          0                    0x132 1019    00d0.040d.380a GE5/3
       45          0                    0xE3  4031    0000.0430.0000 PO4/4
4117   16         0                    0x132 1019    00d0.040d.380a GE5/3*
       17          0                    0xE0  1020    0000.0400.0000 PO4/1
       18          0                    0xE3  4031    0000.0430.0000 PO4/4
4118   21          0                    0xE0  1020    0000.0400.0000 PO4/1*
       56          0                    0xE3  4031    0000.0430.0000 PO4/4
4119   35          0                    0xE3  4031    0000.0430.0000 PO4/4*
       47          0                    0xE0  1020    0000.0400.0000 PO4/1
```

show running interface auto-template

To display configuration information for a tunnel's interface, use the **show running interface auto-template** command in privileged EXEC mode.

show running interface auto-template *num*

Syntax Description

num	Number of the tunnel interface for which you want to display information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The space before the *num* argument is optional.

Examples

The following is output from the **show running interface auto-template** command:

```
Router# show running interface auto-template 1

interface auto-template1
 ip unnumbered Loopback0
 no ip directed-broadcast
 no keepalive
 tunnel destination access-list 1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
```

Table 151 describes the significant fields shown in the display.

Table 151 show running interface auto-template Field Descriptions

Field	Description
ip unnumbered Loopback0	Indicates the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.
no ip directed-broadcast	Indicates that no IP broadcast addresses are used for the autotunnel interface.
no keepalive	Indicates that no keepalives are set for the autotunnel interface.

Table 151 show running interface auto-template Field Descriptions (continued)

Field	Description
tunnel destination access-list 1	Indicates that access list 1 is the access list that the template interface will use for obtaining the autotunnel interface destination address.
tunnel mode mpls traffic-eng	Indicates that the mode of the autotunnel is set to Multiprotocol Label Switching (MPLS) for traffic engineering.
tunnel mpls traffic-eng autoroute announce	Indicates that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.
tunnel mpls traffic-eng path-option 1 dynamic	Indicates that a path option (path-option1) for the label switch router (LSR) for the MPLS traffic engineering (TE) mesh tunnel is configured dynamically.

Related Commands

Command	Description
interface auto-template	Creates the template interface.
tunnel destination access-list	Specifies the access list that the template interface will use for obtaining the mesh tunnel interface destination address.

show running-config vrf

To display the subset of the running configuration of a router that is linked to a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance or to all VRFs configured on the router, use the **show running-config vrf** command in user EXEC or privileged EXEC mode.

show running-config vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) Name of the VRF configuration that you want to display.

Command Default

If you do not specify a *vrf-name* argument, the running configurations of all VRFs on the router are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show running-config vrf** command to display a specific VRF configuration or to display all VRF configurations on the router. To display the configuration of a specific VRF, enter the name of the VRF as an argument to the command.

This command displays the following elements of the VRF configuration:

- The VRF submode configuration
- The routing protocol and static routing configurations associated with the VRF
- The configuration of the interfaces in the VRF, which includes the configuration of any owning controller and physical interface for a subinterface

Examples

The following is sample output from the **show running-config vrf** command. It includes a base VRF configuration for VRF vpn3 and Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) configurations associated with VRF vpn3.

```
Router# show running-config vrf vpn3

Building configuration...

Current configuration : 604 bytes
ip vrf vpn3
 rd 100:3
```

```
 route-target export 100:3
 route-target import 100:3
!
!
interface Loopback1
 ip vrf forwarding vpn3
 ip address 10.43.43.43 255.255.255.255
!
interface Ethernet6/0
 ip vrf forwarding vpn3
 ip address 172.17.0.1 255.0.0.0
 no ip redirects
 duplex half
!
router bgp 100
!
address-family ipv4 vrf vpn3
 redistribute connected
 redistribute ospf 101 match external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 !
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
!
end
```

Table 152 describes the significant fields shown in the display.

Table 152 show running-config vrf Field Descriptions

Field	Description
Current configuration: 604 bytes	Number of bytes (604) in the VRF vpn3 configuration.
ip vrf vpn3	Name of the VRF (vpn3) for which the configuration is displayed.
rd 100:3	Identifies the route distinguisher (100:3) for VRF vpn3.
route-target export 100:3 route-target import 100:3	Specifies the route-target extended community for VRF vpn3. • Routes tagged with route-target export 100:3 are exported from VRF vpn3. • Routes tagged with the route-target import 100:3 are imported into VRF vpn3.
interface Loopback1	Virtual interface associated with VRF vpn3.
ip vrf forwarding vpn3	Associates VRF vpn3 with the named interface.
ip address 10.43.43.43 255.255.255.255	IP address of the loopback interface.
interface Ethernet6/0	Interface associated with VRF vpn3.
ip address 172.17.0.1 255.0.0.0	IP address of the Ethernet interface.

Table 152 show running-config vrf Field Descriptions (continued)

Field	Description
router bgp 100	Sets up a BGP routing process for the router with autonomous system number 100.
address-family ipv4 vrf vpn3	Sets up a routing session for VRF vpn3 using standard IP Version 4 address prefixes.
redistribute connected	Redistributes routes automatically established by IP on an interface into the BGP routing domain.
redistribute ospf 101 match external 1 external 2	Redistribute routes from the OSPF 101 routing domain into the BGP routing domain.
router ospf 101 vrf vpn3	Set up an OSPF routing process and associates VRF vpn3 with OSPF VRF processes.
area 1 sham-link 10.43.43.43 10.23.23.23 cost 10	Configure a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) VPN backbone. • 1 is the ID number of the OSPF area assigned to the sham-link. • 10.43.43.43 is the IP address of the source PE router. • 10.23.23.23 is the IP address of the destination PE router. • 10 is the OSPF cost to send IP packets over the sham-link interface.
network 172.17.0.0 0.255.255.255 area 1	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
show running-config interface	Displays the configuration for a specific interface.

show tech-support mpls

To generate a report of all Multiprotocol Label Switching (MPLS)-related information, use the **show tech-support mpls** command in privileged EXEC mode.

show tech-support mpls [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays MPLS information about the specified VPN routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is useful when you contact technical support personnel with questions regarding MPLS. The **show tech-support mpls** command generates a series of reports. The **show tech-support mpls** command is equivalent to issuing the following commands:

MPLS Forwarding Information Commands

show adjacency detail
show cef drop show cef events
show cef not-cef-switched
show cef state
show interface accounting | exclude sab
show interfaces statistic | exclude sabl
show ip cef adjacency discard
show ip cef adjacency drop
show ip cef adjacency glean
show ip cef adjacency null
show ip cef adjacency punt
show ip cef detail internal
show ip cef inconsistency
show ip cef summary
show ip cef unresolved internal
show ip interfaces
show ip route
show ip traffic
show mpls forwarding-table detail
show mpls interfaces all

show mpls interfaces all internal
show mpls label range
show mpls static binding

MPLS Forwarding: Cell Mode (LC-ATM) Commands

Note These commands are not supported on Cisco 10000 series routers.

show atm vc
show controller vsi descriptor
show controller vsi session
show controller vsi status
show XTagATM cross-connect
show XTagATM cross-connect traffic
show XTagATM vc

MPLS Forwarding: Quality of Service (QoS) Commands

Note These commands are not supported on Cisco 10000 series routers.

show interfaces fair-queue
show interfaces mpls-exp
show interfaces precedence

MPLS Label Distribution Protocol (LDP) Commands

show mpls atm-ldp bindings
show mpls atm-ldp bindwait
show mpls atm-ldp capability
show mpls atm-ldp summary <===== Not supported on Cisco 10000 series routers
show mpls ip binding detail
show mpls ldp backoff
show mpls ldp discovery all detail
show mpls ldp neighbor all
show mpls ldp neighbor detail
show mpls ldp parameters

MPLS LDP: Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart Commands

show mpls checkpoint label-binding
show mpls ldp checkpoint
show mpls ldp graceful-restart
show mpls ldp neighbor graceful-restart

MPLS Traffic Engineering Commands

show ip ospf database opaque-area
show ip ospf database opaque-link
show ip ospf mpls traffic-eng fragment
show ip ospf mpls traffic-eng link
show ip rsvp fast-reroute detail
show ip rsvp installed
show ip rsvp interface

show ip rsvp neighbor
show ip rsvp reservation
show ip rsvp sender
show isis mpls traffic-eng adjacency-log
show isis mpls traffic-eng advertisements
show isis mpls traffic-eng tunnel
show mpls traffic-end link-management interfaces
show mpls traffic-eng autoroute
show mpls traffic-eng fast-reroute database detail
show mpls traffic-eng fast-reroute log reroutes
show mpls traffic-eng forwarding adjacency
show mpls traffic-eng link-management admission-control
show mpls traffic-eng link-management advertisements
show mpls traffic-eng link-management bandwidth-allocation
show mpls traffic-eng link-management summary
show mpls traffic-eng topology
show mpls traffic-eng tunnels
show mpls traffic-eng tunnels brief
show mpls traffic-eng tunnels statics summary

MPLS VPN Commands

show ip bgp labels
show ip bgp neighbors
show ip bgp vpnv4 all
show ip bgp vpnv4 all labels
show ip bgp vpnv4 all summary
show ip vrf detail
show ip vrf interfaces
show ip vrf select

Any Transport over MPLS (AToM) Commands

show mpls l2transport binding
show mpls l2transport hw-capability
show mpls l2transport summary
show mpls l2transport vc detail

MPLS VPN VRF-Specific Commands

show ip bgp vpnv4 *vpn-name* **dampening flap-statistics**
show ip bgp vpnv4 *vpn-name* **labels**
show ip bgp vpnv4 *vpn-name* **peer-group**
show ip bgp vpnv4 *vpn-name* **summary**
show ip bgp vpnv4 vrf *vpn-name* **neighbors**
show ip vrf detail *vpn-name*
show ip vrf interfaces *vpn-name*
show ip vrf select *vpn-name*

MPLS VPN VRF-Specific Forwarding Commands

show ip cef vrf *vpn-name* **adjacency discard**
show ip cef vrf *vpn-name* **adjacency drop**
show ip cef vrf *vpn-name* **adjacency glean**
show ip cef vrf *vpn-name* **adjacency null**
show ip cef vrf *vpn-name* **adjacency punt**

show ip cef vrf *vpn-name* **inconsistency**
show ip cef vrf *vpn-name* **internal**
show ip cef vrf *vpn-name* **summary**
show ip route vrf *vpn-name*
show ip vrf interfaces *vpn-name*
show mpls forwarding-table vrf *vpn-name*
show mpls interface vrf*vpn-name* **detail**

MPLS LDP VRF-Specific Commands

show mpls ip binding vrf *vpn-name* **atm detail**
show mpls ip binding vrf *vpn-name* **detail**
show mpls ip binding vrf *vpn-name* **local**
show mpls ip binding vrf *vpn-name* **summary**
show mpls ldp discovery vrf *vpn-name* **detail**
show mpls ldp neighbor vrf *vpn-name* **detail**

MPLS LDP VRF Graceful Restart-Specific Commands

show mpls ldp neighbor vrf *vpn-name* **graceful-restart**

These commands are documented in individual feature modules or Cisco IOS Release 12.2 command references. Refer to the individual commands for information about the output these commands generate.

Examples

The following example displays an abbreviated version of the **show tech-support mpls** command output:

```
Router# show tech-support mpls

------------------ show version ------------------

Cisco IOS Software, 7300 Software (C7300-P-M), Version 12.2(27)SBC, RELEASE SOF)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sat 10-Sep-05 17:44 by ssearch
.
.
.
------------------ show running-config ------------------

Building configuration...
```

```
Current configuration : 1827 bytes
.
.
.
------------------ show mpls ldp graceful-restart ------------------

LDP Graceful Restart is disabled
Neighbor Liveness Timer: 120 seconds
Max Recovery Time: 120 seconds
Forwarding State Holding Time: 600 seconds
```

Related Commands

Command	Description
show tech-support	Displays the equivalent of the **show buffers**, **show controllers**, **show interfaces**, **show process**, **show process memory**, **show running-config**, **show stacks**, and **show version** commands.

show vrf

To display the defined Virtual Private Network (VPN) routing and forwarding (VRF) instances, use the **show vrf** command in user EXEC or privileged EXEC mode.

show vrf [**ipv4** | **ipv6**] [**interface** | **brief** | **detail** | **id** | **select** | **lock**] [*vrf-name*]

Syntax Description

ipv4	(Optional) Displays IPv4 address-family type VRF instances.
ipv6	(Optional) Displays IPv6 address-family type VRF instances.
interface	(Optional) Displays the interface associated with the specified VRF instances.
brief	(Optional) Displays brief information about the specified VRF instances.
detail	(Optional) Displays detailed information about the specified VRF instances.
id	(Optional) Displays VPN-ID information for the specified VRF instances.
select	(Optional) Displays selection information for the specified VRF instances.
lock	(Optional) Displays VPN lock information for the specified VRF instances.
vrf-name	(Optional) Name assigned to a VRF.

Command Default

If you do not specify any arguments or keywords, the command displays concise information about all configured VRFs.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. When backup paths have been created either through the Prefix Independent Convergence or Best External feature, the output of the **show vrf detail** command displays the following line: `Prefix protection with additional path enabled`

Usage Guidelines

Use the **show vrf** command to display information about specified VRF instances or all VRF instances. Specify no arguments or keywords to display information on all VRF instances.

Examples

The following is the sample output from the **show vrf** command that displays brief information about all configured VRF instances:

```
Router# show vrf

  Name                              Default RD          Protocols   Interfaces
  N1                                100:0               ipv4,ipv6
  V1                                1:1                 ipv4        Lo1
  V2                                2:2                 ipv4,ipv6   Et0/1.1
                                                                    Et0/1.2
                                                                    Et0/1.3
  V3                                3:3                 ipv4        Lo3
                                                                    Et0/1.4
```

Table 153 describes the significant fields shown in the display.

Table 153 show vrf Field Descriptions

Field	Description
Name	Name of the VRF instance.
Default RD	The default route distinguisher (RD) for the specified VRF instances.
Protocols	The address-family protocol type for the specified VRF instance.
Interfaces	The network interface associated with the VRF instance.

The following example displays output from the **show vrf** command with the **detail** keyword. The information shown is for a VRF named cisco1.

```
Router# show vrf detail

VRF cisco1; default RD 100:1; default VPNID <not set>
  Interfaces:
    Ethernet0/0                 Loopback10
Address family ipv4 (Table ID = 0x1):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
Address family ipv6 (Table ID = 0xE000001):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

Table 154 describes the significant fields shown in the display.

Table 154 show vrf detail Field Descriptions

Field	Description
default RD 100:1	The RD given to this VRF.
Interfaces:	Interfaces to which the VRF is attached.
Export VPN route-target communities RT:100:1	Route-target VPN extended communities to be exported.
Import VPN route-target communities RT:100:1	Route-target VPN extended communities to be imported.

The following example displays output from the **show vrf detail** command when backup paths have been created either through the Prefix Independent Convergence or Best External feature. The output of the **show vrf detail** command displays the following line:

```
Prefix protection with additional path enabled
```

```
Router# show vrf detail

VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    Et1/1
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
  Prefix protection with additional path enabled
Address family ipv6 not active.
```

The following is the sample output from the **show vrf lock** command that displays VPN lock information:

```
Router# show vrf lock

VRF Name: Mgmt-intf; VRF id = 4085 (0xFF5)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :108
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
VRF Name: vpn1; VRF id = 1 (0x1)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :100
```

```
Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
Caller PC tracebacks:
Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
```

Related Commands

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.
vrf forwarding	Associates a VRF instance with an interface or subinterface.

show xconnect

To display information about xconnect attachment circuits and pseudowires, use the **show xconnect** command in user EXEC or privileged EXEC mode.

show xconnect {{**all** | **interface** *type number*} [**detail**] | **peer** *ip-address* {**all** | **vcid** *vcid-value*} [**detail**] | **pwmib** [**peer** *ip-address vcid-value*]}

Cisco IOS SR Train

show xconnect {{**all** | **interface** *type number* | **memory** | **rib**} [**detail**] | **peer** *ip-address* {**all** | **vcid** *vcid-value*} [**detail**] | **pwmib** [**peer** *ip-address vcid-value*]}

Cisco uBR10012 Router and Cisco uBR7200 Series Universal Broadband Routers

show xconnect {**all** | **peer** *ip-address* {**all** | **vcid** *vcid*} | **pwmib** [**peer** ip-address vcid]} [**detail**]

Syntax Description

all	Displays information about all xconnect attachment circuits and pseudowires.
interface	Displays information about xconnect attachment circuits and pseudowires on the specified interface.
type	Interface type. For more information, use the question mark (?) online help function. Valid values for the *type* argument are as follows: **atm** *number*—Displays xconnect information for a specific ATM interface or subinterface. **atm** *number* **vp** *vpi-value*—Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). This command will not display information about virtual circuit (VC) xconnects using the specified VPI. **atm** *number* **vp** *vpi-value*/*vci-value*—Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination. **ethernet** *number*—Displays port-mode xconnect information for a specific Ethernet interface or subinterface. **fastethernet** *number*—Displays port-mode xconnect information for a specific Fast Ethernet interface or subinterface. **serial** *number*—Displays xconnect information for a specific serial interface. **serial** *number dlci-number*—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed information about the specified xconnect attachment circuits and pseudowires.
peer	Displays information about xconnect attachment circuits and pseudowires associated with the specified peer.
ip-address	Specifies the IP address of the peer.

all	Displays all xconnect information associated with the specified peer IP address.
vcid	Displays xconnect information associated with the specified peer IP address and the specified VC ID.
vcid-value	Specifies the VC ID value.
pwmib	Displays information about pseudowires Management Information Base (MIB).
memory	Displays information about the xconnect memory usage.
rib	Displays information about the pseudowire Routing Information Base (RIB).
pwmib	Displays MIB information for all xconnect attachment circuits and pseudowires.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was modified. The **rib** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **pwmib** keyword was added.
12.2(33)SRC	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SRC. The **memory** keyword was added.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

The **show xconnect** command can be used to display, sort, and filter basic information about all xconnect attachment circuits and pseudowires.

You can use the **show xconnect** command output to help determine the appropriate steps required to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the “Related Commands” table.

Examples

The following example shows **show xconnect all** command output in the brief (default) display format:

```
Router# show xconnect all

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, SB=Standby, RV=Recovering, NH=No Hardware
XC ST     Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
UP     ac   Se7/0(PPP)                   UP mpls 10.55.55.2:2175              UP
UP pri ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.2:2230              UP
IA sec ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.3:2231              DN
UP     ac   Se4/0(HDLC)                  UP mpls 10.55.55.2:4000              UP
UP     ac   Se6/0:500(FR DLCI)           UP l2tp 10.55.55.2:5000              UP
UP     ac   Et1/0.1:200(Eth VLAN)        UP mpls 10.55.55.2:5200              UP
UP pri ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.2:5225              UP
IA sec ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.3:5226              DN
IA pri ac   Et1/0.2:100(Eth VLAN)        UP ac   Et2/0.2:100(Eth VLAN)        UP
UP sec ac   Et1/0.2:100(Eth VLAN)        UP mpls 10.55.55.3:1101              UP
UP     ac   Se6/0:150(FR DLCI)           UP ac   Se8/0:150(FR DLCI)           UP
```

The following example shows **show xconnect all** command output in the detailed display format:

```
Router# show xconnect all detail

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, SB=Standby, RV=Recovering, NH=No HardwareXC
ST     Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
            Interworking: ip                      Local VC label 16
                                                  Remote VC label 16
                                                  pw-class: mpls-ip
UP     ac   Se7/0(PPP)                   UP mpls 10.55.55.2:2175              UP
            Interworking: ip                      Local VC label 22
                                                  Remote VC label 17
                                                  pw-class: mpls-ip
UP pri ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.2:2230              UP
            Interworking: ip                      Local VC label 21
                                                  Remote VC label 18

pw-class: mpls-ip
IA sec ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.3:2231              DN
            Interworking: ip                      Local VC label unassigned
                                                  Remote VC label 19
                                                  pw-class: mpls-ip
SB ac   Se4/0:100(FR DLCI)           UP mpls 10.55.55.2:4000              SB
            Interworking: none                    Local VC label 18
                                                  Remote VC label 19
                                                  pw-class: mpls
UP     ac   Se6/0:500(FR DLCI)           UP l2tp 10.55.55.2:5000              UP
            Interworking: none                    Session ID: 34183
                                                  Tunnel ID: 62083
                                                  Peer name: pe-iou2
                                                  Protocol State: UP
                                                  Remote Circuit State: UP
                                                  pw-class: l2tp
UP     ac   Et1/0.1:200(Eth VLAN)        UP mpls 10.55.55.2:5200              UP
            Interworking: ip                      Local VC label 17
                                                  Remote VC label 20
                                                  pw-class: mpls-ip
UP pri ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.2:5225              UP
            Interworking: none                    Local VC label 19
                                                  Remote VC label 21
                                                  pw-class: mpls
```

```
IA sec ac   Se6/0:225(FR DLCI)          UP mpls 10.55.55.3:5226             DN
            Interworking: none                  Local VC label unassigned
                                                Remote VC label 22
                                                pw-class: mpls
IA pri ac   Et1/0.2:100(Eth VLAN)       UP ac   Et2/0.2:100(Eth VLAN)       UP
            Interworking: none                  Interworking: none
UP sec ac   Et1/0.2:100(Eth VLAN)       UP mpls 10.55.55.3:1101             UP
            Interworking: none                  Local VC label 23
                                                Remote VC label 17
                                                pw-class: mpls
UP     ac   Se6/0:150(FR DLCI)          UP ac   Se8/0:150(FR DLCI)          UP
            Interworking: none                  Interworking: none
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Brief Display Format

The following is a sample output of the **show xconnect** command in the brief (default) display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router:

```
Router# show xconnect all

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware

XC ST  Segment 1                        S1 Segment 2                        S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Bu254:2001(DOCSIS)          UP mpls 10.76.1.1:2001              UP
UP     ac   Bu254:2002(DOCSIS)          UP mpls 10.76.1.1:2002              UP
UP     ac   Bu254:2004(DOCSIS)          UP mpls 10.76.1.1:2004              UP
DN     ac   Bu254:22(DOCSIS)            UP mpls 101.1.0.2:22                DN
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Detailed Display Format

The following is a sample output of the **show xconnect** command in the detailed display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router:

```
Router# show xconnect all detail

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware

XC ST  Segment 1                        S1 Segment 2                        S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Bu254:2001(DOCSIS)          UP mpls 10.76.1.1:2001              UP
            Interworking: ethernet              Local VC label 40
                                                Remote VC label 110
                                                pw-class:
UP     ac   Bu254:2002(DOCSIS)          UP mpls 10.76.1.1:2002              UP
            Interworking: ethernet              Local VC label 41
                                                Remote VC label 88
                                                pw-class:
UP     ac   Bu254:2004(DOCSIS)          UP mpls 10.76.1.1:2004              UP
            Interworking: ethernet              Local VC label 42
                                                Remote VC label 111
                                                pw-class:
DN     ac   Bu254:22(DOCSIS)            UP mpls 101.1.0.2:22                DN
            Interworking: ethernet              Local VC label 39
                                                Remote VC label unassigned
                                                pw-class:
```

Table 155 describes the significant fields shown in the display.

Table 155 show xconnect all Field Descriptions

Field	Description
XC ST	State of the xconnect attachment circuit or pseudowire. Valid states are: • DN—The xconnect attachment circuit or pseudowire is down. Either segment 1, segment 2, or both segments are down. • IA—The xconnect attachment circuit or pseudowire is inactive. This state is valid only when pseudowire redundancy is configured. • NH—One or both segments of this xconnect no longer have the required hardware resources available to the system. • UP—The xconnect attachment circuit or pseudowire is up. Both segment 1 and segment 2 must be up for the xconnect to be up.
Segment1 or Segment2	Information about the type of xconnect, the interface type, and the IP address the segment is using. Types of xconnects are as follows: • ac—Attachment circuit • l2tp—Layer 2 Tunnel Protocol • mpls—Multiprotocol Label Switching • pri ac—Primary attachment circuit • sec ac—Secondary attachment circuit
S1 or S2	State of the segment. Valid states are: • AD—The segment is administratively down. • DN—The segment is down. • HS—The segment is in hot standby mode. • RV—The segment is recovering from a graceful restart. • SB—The segment is in a standby state. • UP—The segment is up.

The additional fields displayed in the detailed output are self-explanatory.

For VPLS Autodiscovery, issuing the **show xconnect** command with the **rib** keyword provides RIB detail, as shown in the following:

```
Router# show xconnect rib

Local Router ID: 10.9.9.9

Legend: O=Origin, P=Provisioned, TID=Target ID, B=BGP, Y=Yes, N=No
O P  VPLS/VPWS-ID         TID        Next-Hop        Route-Target
-+-+--------------------+-----------+---------------+--------------------
B Y 10:123                10.7.7.7     10.7.7.7         10:123
B N 10:123                10.7.7.8     10.7.7.8         10:123
B Y 10.100.100.100:1234   10.0.0.2     10.2.2.2         10.111.111.111:12345
                                       10.3.3.3         10.8.8.8:345
                                       10.4.4.4
B Y 128.100.100.100:1234  10.13.1.1    10.1.1.1         10.111.111.111:12345
```

Table 156 describes the significant fields shown in the display.

Table 156 show xconnect rib Field Descriptions

Field	Description
Local Router ID	A unique router identifier. VPLS Autodiscovery automatically generates a router ID using the MPLS global router ID.
O	The origin of the route.
P	Whether the pseudowire has been provisioned using a learned route.
VPLS/WPWS-ID	The Virtual Private LAN Service (VPLS) domain. VPLS Autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) autonomous system number and the configured VFI VPN ID.
TID	The target ID. The IP address of the destination router.
Next-Hop	The IP address of the next hop router.
Route-Target	The route target (RT). VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPLS ID.

For VPLS Autodiscovery, issuing the **show xconnect** command with the **rib** and **detail** keywords provides more information about the routing information base, as shown in the following example:

```
Router# show xconnect rib detail

Local Router ID: 10.9.9.9

VPLS-ID 10:123, TID 10.7.7.7
  Next-Hop: 10.7.7.7
  Hello-Source: 10.9.9.9
  Route-Target: 10:123
  Incoming RD: 10:10
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: Yes
VPLS-ID 10:123, TID 10.7.7.8
  Next-Hop: 10.7.7.8
  Hello-Source: 10.9.9.9
```

```
  Route-Target: 10:123
  Incoming RD: 10:11
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: No
VPLS-ID 10.100.100.100:1234, TID 0.0.0.2
  Next-Hop: 10.2.2.2, 10.3.3.3, 10.4.4.4
  Hello-Source: 10.9.9.9
  Route-Target: 10.111.111.111:12345, 10.8.8.8:345
  Incoming RD: 10:12
  Forwarder: vfi VPLS2
  Origin: BGP
  Provisioned: Yes
VPLS-ID 10.100.100.100:1234, TID 10.13.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.9.9.9
  Route-Target: 10.111.111.111:12345
  Incoming RD: 10:13
  Forwarder: vfi VPLS2
  Origin: BGP
  Provisioned: Yes
```

Table 157 describes the significant fields shown in the display.

Table 157 show xconnect rib detail Field Descriptions

Field	Description
Hello-Source	The source IP address used when Label Distribution Protocol (LDP) hello messages are sent to the LDP peer for the autodiscovered pseudowire.
Incoming RD	The route distinguisher for the autodiscovered pseudowire.
Forwarder	The VFI to which the autodiscovered pseudowire is attached.

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.
show atm vc	Displays all ATM PVCs and SVCs and traffic information.
show atm vp	Displays the statistics for all VPs on an interface or for a specific VP.
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show l2tun session	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
show mpls l2transport binding	Displays VC label binding information.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

show xtagatm cos-bandwidth-allocation

Note Effective with Cisco IOS Release 12.4(20)T, the **show xtagatm cos-bandwidth-allocation** command is not available in Cisco IOS software.

To display information about quality of service (QoS) bandwidth allocation on extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interfaces, use the **show xtagatm cos-bandwidth-allocation** command in user EXEC or privileged EXEC mode.

show xtagatm cos-bandwidth-allocation [**xtagatm** *interface-number*]

Syntax Description

xtagatm	(Optional) Specifies the XTagATM interface number.
interface-number	Number of the XTagATM interface. Range: 0 to 2147483647.

Defaults

Available 50 percent, control 50 percent.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

Use this command to display QoS bandwidth allocation information for the following QoS traffic categories:

- Available
- Standard
- Premium
- Control

Examples

The following example shows output from this command:

```
Router# show xtagatm cos-bandwidth-allocation xtagatm 123

CoS             Bandwidth allocation
available       25%
standard        25%
premium         25%
control         25%
```

Table 158 describes the significant fields shown in the display.

Table 158 show xtagatm cos-bandwidth-allocation Field Descriptions

Field	Description
CoS	Class of service for transmitted packets.
Bandwidth Allocation	Percentage bandwidth allocated to each QoS traffic category.

show xtagatm cross-connect

Note Effective with Cisco IOS Release 12.4(20)T, the **show xtagatm cross-connect** command is not available in Cisco IOS software.

To display information about the Label Switch Controller (LSC) view of the cross-connect table on the remotely controlled ATM switch, use the **show xtagatm cross-connect** command in user EXEC or privileged EXEC mode.

show xtagatm cross-connect [*traffic*] [**interface** *interface* [*vpi vci*] | **descriptor** *descriptor* [*vpi vci*]]

Syntax Description

traffic	(Optional) Displays receive and transmit cell counts for each connection.
interface *interface*	(Optional) Displays only connections with an endpoint of the specified interface.
vpi vci	(Optional) Displays only detailed information on the endpoint with the specified virtual path identifier (VPI)/virtual channel identifier (VCI) on the specified interface.
descriptor *descriptor*	(Optional) Displays only connections with an endpoint on the interface with the specified physical descriptor.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

Examples

Each connection is listed twice in the output from the **show xtagatm cross-connect** command, because it shows each interface that is linked by the connection.

The following is sample output from the **show xtagatm cross-connect** command:

```
Router# show xtagatm cross-connect

Phys Desc    VPI/VCI     Type   X-Phys Desc  X-VPI/VCI   State

10.1.0       1/37        ->     10.3.0       1/35        UP
10.1.0       1/34        ->     10.3.0       1/33        UP
10.1.0       1/33        <->    10.2.0       0/32        UP
10.1.0       1/32        <->    10.3.0       0/32        UP
10.1.0       1/35        <-     10.3.0       1/34        UP
10.2.0       1/57        ->     10.3.0       1/49        UP
10.2.0       1/53        ->     10.3.0       1/47        UP
10.2.0       1/48        <-     10.1.0       1/50        UP
10.2.0       0/32        <->    10.1.0       1/33        UP
10.3.0       1/34        ->     10.1.0       1/35        UP
```

```
10.3.0       1/49        <-     10.2.0       1/57        UP
10.3.0       1/47        <-     10.2.0       1/53        UP
10.3.0       1/37        <-     10.1.0       1/38        UP
10.3.0       1/35        <-     10.1.0       1/37        UP
10.3.0       1/33        <-     10.1.0       1/34        UP
10.3.0       0/32        <->    10.1.0       1/32        UP
```

Table 159 describes the significant fields shown in the display.

Table 159 show xtagatm cross-connect Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
Type	The type can be one of the following: A right arrow (->) indicates an ingress endpoint, where traffic is received into the switch. A left arrow (<-) indicates an egress endpoint, where traffic is transmitted from the interface. A bidirectional arrow (<->) indicates that traffic is both transmitted and received at this endpoint.
X-Phys Desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.
State	Indicates the status of the cross-connect to which this endpoint belongs. The state is typically UP; other values, all of which are transient, include the following: • DOWN • ABOUT_TO_DOWN • ABOUT_TO_CONNECT • CONNECTING • ABOUT_TO_RECONNECT • RECONNECTING • ABOUT_TO_RESYNC • RESYNCING • NEED_RESYNC_RETRY • ABOUT_TO_RESYNC_RETRY RETRYING_RESYNC • ABOUT_TO_DISCONNECT • DISCONNECTING

The following is sample output from the **show xtagatm cross-connect** command for a single endpoint:

```
Router# show xtagatm cross-connect descriptor 10.1.0 1 42
```

```
Phys desc:   10.1.0
Interface:   n/a
Intf type:   switch control port
VPI/VCI:     1/42
X-Phys desc: 10.2.0
X-Interface: XTagATM0
X-Intf type: extended tag ATM
X-VPI/VCI:   2/38
Conn-state:  UP
Conn-type:   input/output
Cast-type:   point-to-point
Rx service type:   Tag COS 0
Rx cell rate:      n/a
Rx peak cell rate: 10000
Tx service type:   Tag COS 0
Tx cell rate:      n/a
Tx peak cell rate: 10000
```

Table 160 describes the significant fields shown in the display.

Table 160 show xtagatm cross-connect descriptor Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
Interface	The (Cisco IOS) interface name.
Intf type	Interface type. Can be either extended Multiprotocol Label Switched (MPLS) ATM (XTagATM) or a switch control port.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
X-Phys desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-Interface	The (Cisco IOS) name for the interface of the other endpoint belonging to the cross-connect.
X-Intf type	Interface type for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.

Table 160 show xtagatm cross-connect descriptor Field Descriptions (continued)

Field	Description
Conn-state	Indicates the status of the cross-connect to which this endpoint belongs. The cross-connect state is typically UP; other values, all of which are transient, include the following: • DOWN ABOUT_TO_DOWN ABOUT_TO_CONNECT • CONNECTING • ABOUT_TO_RECONNECT • RECONNECTING • ABOUT_TO_RESYNC • RESYNCING • NEED_RESYNC_RETRY • ABOUT_TO_RESYNC_RETRY • RETRYING_RESYNC • ABOUT_TO_DISCONNECT • DISCONNECTING
Conn-type	Input—Indicates an ingress endpoint where traffic is only expected to be received into the switch. Output—Indicates an egress endpoint, where traffic is only expected to be sent from the interface. Input/output—Indicates that traffic is expected to be both send and received at this endpoint.
Cast-type	Indicates whether the cross-connect is multicast.
Rx service type	Quality of service type for the receive, or ingress, direction. This is MPLS QoS <*n*>, (MPLS Quality of Service <*n*>), where *n* is in the range from 0 to 7 for input and input/output endpoints; this will be N/A for output endpoints. (In the first release, this is either 0 or 7.)
Rx cell rate	(Guaranteed) cell rate in the receive, or ingress, direction.
Rx peak cell rate	Peak cell rate in the receive, or ingress, direction, in cells per second. This is n/a for an output endpoint.
Tx service type	Quality of service type for the transmit, or egress, direction. This is MPLS QoS <*n*>, (MPLS Class of Service <*n*>), where *n* is in the range from 0 to 7 for output and input/output endpoints; this will be N/A for input endpoints.
Tx cell rate	(Guaranteed) cell rate in the transmit, or egress, direction.
Tx peak cell rate	Peak cell rate in the transmit, or egress, direction, in cells per second. This is N/A for an input endpoint.

show xtagatm vc

Note Effective with Cisco IOS Release 12.4(20)T, the **show xtagatm vc** command is not available in Cisco IOS software.

To display information about terminating virtual circuits (VCs) on extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interfaces, use the **show xtagatm vc** command in user EXEC or privileged EXEC mode.

show xtagatm vc [*vcd* [*interface*]]

Syntax Description

vcd	(Optional) Virtual circuit descriptor (virtual circuit number). If you specify the *vcd* argument, information displays about all VCs with that virtual circuit descriptor (VCD). If you do not specify the *vcd* argument, a summary description of all VCs on all XTagATM interfaces displays.
interface	(Optional) Interface number. If you specify the *interface* and the *vcd* arguments, information displays about the specified VC on the specified interface.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modifications
12.0(5)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

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.

Examples

Each connection is listed twice in the sample output from the **show xtagatm vc** command under each interface that is linked by the connection. Connections are marked as input (unidirectional traffic flow, into the interface), output (unidirectional traffic flow, away from the interface), or in/out (bidirectional).

The following is sample output from the **show xtagatm vc** command:

```
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
```

Table 161 describes the significant fields shown in the display.

Table 161 show xtagatm vc Field Descriptions

Field	Description
VCD	Virtual circuit descriptor (virtual circuit number).
VPI	Virtual path identifier.
VCI	Virtual circuit identifier.
Control Interf. VCD	VCD for the corresponding private VC on the control interface.
Control Interf. VPI	VPI for the corresponding private VC on the control interface.
Control Interf. VCI	VCI for the corresponding private VC on the control interface.
Encapsulation	Displays the type of connection on the interface.
Status	Displays the current state of the specified ATM interface.

Related Commands

Command	Description
show atm vc	Displays information about private ATM VCs.
show xtagatm cross-connect	Displays information about remotely connected ATM switches.

snmp mib mpls vpn

To configure Simple Network Management Protocol (SNMP) controls for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) notification thresholds, use the **snmp mib mpls vpn** command in global configuration mode. To disable SNMP controls for MPLS VPN thresholds, use the **no** form of this command.

snmp mib mpls vpn {**illegal-label** *number* | **max-threshold** *seconds*}

no snmp mib mpls vpn {**illegal-label** | **max-threshold**}

Syntax Description

illegal-label	Controls MPLS VPN illegal label threshold exceeded notifications.
number	Number of illegal labels allowed before SNMP sends an illegal label threshold notification. The valid range is from 1 to 4,294,967,295. The default is 0.
max-threshold	Controls MPLS VPN maximum threshold exceeded notifications.
seconds	Time in seconds before SNMP resends maximum threshold notifications. The valid range is from 0 to 4,294,967,295. The default is 0.

Command Default

SNMP controls are not configured for MPLS VPN routing and forwarding (VRF) tables.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to configure the number of illegal labels allowed for routes in the MPLS VRF before SNMP sends an illegal label threshold notification, or to configure the time elapsed before SNMP resends a maximum threshold notification.

Use the **snmp mib mpls vpn illegal-label** command to indicate how many illegal MPLS VPN labels you want to allow before you receive a notification. Once this number is exceeded, SNMP sends an illegal-label notification to a network management system (NMS), if you have one configured; otherwise, the router issues a syslog error message. If you do not configure this command, SNMP sends an illegal label notification on the first occurrence of an illegal label.

Use the **snmp mib mpls vpn max-threshold** command if you want to receive maximum threshold notifications periodically when attempts are made to add routes to the VRF after the maximum threshold is exceeded. If you do not configure this command, SNMP sends a single maximum threshold notification at the time that the maximum threshold is exceeded. Notifications are sent to an NMS if you configured one; otherwise, the router issues a syslog error message. Another notification is not sent until the number of routes goes below the maximum threshold and then exceeds the threshold again.

Examples

The following example shows how to configure an illegal label threshold of 50 labels:

```
configure terminal
!
smnp mib mpls vpn illegal-label 50
```

The following example shows how to configure the time interval of 600 seconds for resending maximum threshold notifications:

```
configure terminal
!
smnp mib mpls vpn max-threshold 600
```

Related Commands

Command	Description
ip vrf	Specifies a name for a VRF routing table and enters VRF configuration mode (for IPv4 VRF only).
maximum routes	Limits the maximum number of routes in a VRF to prevent a PE router from importing too many routes.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]

no snmp-server community *string*

Syntax Description

string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
view-name	(Optional) Name of a previously defined view.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
ipv6	(Optional) Specifies an IPv6 named access list.
nacl	(Optional) IPv6 named access list.
access-list-number	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Command Default

An SNMP community string permits read-only access to all objects.

Note If the **snmp-server community** command is not used during the SNMP configuration session, the command will automatically be added to the configuration after the **snmp host** command is used. In this case, the default password (*string*) for the **snmp-server community** command will be taken from the **snmp host** command.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The **ipv6** *nacl* keyword and argument pair was added to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The **ipv6** *nacl* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword and argument pair is not supported in Cisco IOS 12.2S releases.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).

The **snmp-server community** command can be used to specify only an IPv6 named access list, only an IPv4 access list, or both. For you to configure both IPv4 and IPv6 access lists, the IPv6 access list must appear first in the command statement.

Note The @ symbol is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to allow read-only access for all objects to members of the standard named access list lmnop that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro lmnop
```

The following example shows how to assign the string comaccess to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string manager to SNMP and allow read-write access to the objects in the restricted view:

```
Router(config)# snmp-server community manager view restricted rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

The following example shows how to configure an IPv6 access list named list1 and links an SNMP community string with this access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 list1
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
snmp-server enable traps	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.
snmp-server view	Creates or updates a view entry.

snmp-server enable traps (MPLS)

To enable a label switch router (LSR) to send Simple Network Management Protocol (SNMP) notifications or informs to an SNMP host, use the **snmp-server enable traps** command in global configuration mode. To disable notifications or informs, use the **no** form of this command.

snmp-server enable traps [*notification-type*] [*notification-option*]

no snmp-server enable traps [*notification-type*] [*notification-option*]

Syntax Description

notification-type	(Optional) Specifies the particular type of SNMP notification(s) to be enabled on the LSR. If a notification type is not specified, all SNMP notifications applicable to the LSR are enabled and sent to the SNMP host. Any one or all of the following keywords can be specified in any combination as the *notification-type* (family name) in the **snmp-server enable traps** command: • **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. • **config**—Sends configuration notifications. • **entity**—Sends entity MIB modification notifications. • **envmon**—Sends Cisco enterprise-specific environmental monitor notifications whenever certain environmental thresholds are exceeded. *Notification-option* arguments (below) can be specified in combination with this keyword. • **frame-relay**—Sends Frame Relay notifications. • **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications. • **isdn**—Sends ISDN notifications. *Notification-option* arguments (see examples below) can be specified in combination with this keyword. • **repeater**—Sends Ethernet repeater (hub) notifications. *Notification-option* arguments (see examples below) can be specified in combination with this keyword. • **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications. • **rtr**—Sends Service Assurance Agent/Response Time Reporter (RTR) notifications. • **snmp** [**authentication**]—Sends RFC 1157 SNMP notifications. Using the **authentication** keyword produces the same effect as not using it. Both the **snmp-server enable traps snmp** and the **snmp-server enable traps snmp authentication** forms of this command globally enable the following SNMP notifications (or, if you are using the **no** form of the command, disables such notifications): **authenticationFailure**, **linkUp**, **linkDown**, and **warmstart**. • **syslog**—Sends system error message (syslog) notifications. You can specify the level of messages to be sent using the **logging history level** command.

notification-type (continued)	• **mpls ldp**—Sends notifications about status changes in LDP sessions. Note that this keyword is specified as ***mpls ldp***. This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with this keyword. • **mpls traffic-eng**—Sends notifications about status changes in MPLS label distribution tunnels. This keyword is specified as ***mpls traffic-eng***. This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with this keyword.
notification-option	(Optional) Defines the particular options associated with the specified *notification-type* that are to be enabled on the LSR. • **envmon** [**voltage** | **shutdown** | **supply** | **fan** | **temperature**] When you specify the **envmon** keyword, you can enable any one or all of the following environmental notifications in any combination: **voltage**, **shutdown**, **supply**, **fan**, or **temperature**. If you do not specify an argument with the **envmon** keyword, all types of system environmental notifications are enabled on the LSR. • **isdn** [**call-information** | **isdn u-interface**] When you specify the **isdn** keyword, you can use either the **call-information** argument (to enable an SNMP ISDN call information option for the ISDN MIB subsystem) or the **isdn u-interface** argument (to enable an SNMP ISDN U interface option for the ISDN U Interfaces MIB subsystem), or both. If you do not specify an argument with the **isdn** keyword, both types of isdn notifications are enabled on the LSR. • **repeater** [**health** | **reset**] When you specify the **repeater** keyword, you can use either the **health** argument or the **reset** argument, or both (to enable the IETF Repeater Hub MIB [RFC 1516] notification). If you do not specify an argument with the **repeater** keyword, both types of notifications are enabled on the LSR. • **mpls ldp** [**session-up** | **session-down** | **pv-limit** | **threshold**] When you specify the **mpls ldp** keyword, you can use any one or all of the following arguments in any combination to indicate status changes in LDP sessions: **session-up**, **session-down**, **pv-limit**, or **threshold**. If you do not specify an argument with the **mpls ldp** keyword, all four types of LDP session notifications are enabled on the LSR. • **mpls traffic-eng** [**up** | **down** | **reroute**] When you specify the **mpls traffic-eng** keyword, you can use any one or all of the following arguments in any combination to enable the sending of notifications regarding status changes in MPLS label distribution tunnels: **up**, **down**, or **reroute**. If you do not specify an argument with the **mpls traffic-eng** keyword, all three types of tunnel notifications are enabled on the LSR.

Defaults

If you issue this command on an LSR without specifying any *notification-type* keywords, the default behavior of the LSR is to enable all notification types controlled by the command (some notification types cannot be controlled by means of this command).

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	The **snmp-server enable traps snmp authentication** form of this command was introduced to replace the **snmp-server trap-authentication** command.
12.0(17)ST	The **mpls traffic-eng** keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type* and *notification-option* parameters of the **snmp-server enable traps** command.
12.0(21)ST	The **mpls ldp** keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type* and *notification-option* parameters of the **snmp-server enable traps** command.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To configure an LSR to send SNMP LDP notifications, you must issue at least one **snmp-server enable traps** command on the router.

To configure an LSR to send either notifications (traps) or informs to a designated network management station (NMS), you must issue the **snmp-server host** command on that device, using the keyword (**traps** or **informs**) that suits your purposes.

If you issue the **snmp-server enable traps** command without keywords, all SNMP notification types are enabled on the LSR. If you issue this command with specific keywords, only the notification types associated with those particular keywords are enabled on the LSR.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. You use the latter command to specify the NMS host (or hosts) targeted as the recipient(s) of the SNMP notifications generated by SNMP-enabled LSRs in the network. To enable an LSR to send such notifications, you must issue at least one **snmp-server host** command on the LSR.

Examples

In the following example, the router is enabled to send all notifications to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps

Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, the router is enabled to send Frame Relay and environmental monitor notifications to the host specified as myhost.cisco.com. The community string is defined as public:

```
Router(config)# snmp-server enable traps frame-relay

Router(config)# snmp-server enable traps envmon temperature

Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, notifications are not sent to any host. BGP notifications are enabled for all hosts, but the only notifications enabled to be sent to a host are ISDN notifications (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp

Router(config)# snmp-server host host1 public isdn
```

In the following example, the router is enabled to send all inform requests to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps

Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

In the following example, HSRP MIB notifications are sent to the host specified as myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable hsrp

Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Related Commands

Command	Description
snmp-server host	Specifies the intended recipient of an SNMP notification (that is, the designated NMS workstation in the network).

snmp-server enable traps mpls ldp

To enable the sending of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps mpls ldp** command in global configuration mode. To disable the sending of MPLS LDP notifications, use the **no** form of this command.

snmp-server enable traps mpls ldp [**pv-limit**] [**session-down**] [**session-up**] [**threshold**]

no snmp-server enable traps mpls ldp [**pv-limit**] [**session-down**] [**session-up**] [**threshold**]

Syntax Description

pv-limit	(Optional) Enables or disables path-vector (PV) limit notifications (mplsLdpPathVectorLimitMismatch).
session-down	(Optional) Enables or disables LDP session down notifications (mplsLdpSessionDown).
session-up	(Optional) Enables or disables LDP session up notifications (mplsLdpSessionUp).
threshold	(Optional) Enables or disables PV Limit notifications (mplsLdpFailedInitSessionThresholdExceeded).

Command Default

The sending of SNMP notifications is disabled. If you do not specify an optional keyword, all four types of LDP notifications are enabled on the label switching router (LSR).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The MPLS LDP pv-limit (mplsLdpPathVectorLimitMismatch) notification provides a warning message that can be sent to the network management station (NMS) when two routers engaged in LDP operations have a dissimilar path-vector limits.

The value of the path-vector limit can range from 0 to 255; a value of 0 indicates that loop detection is off. Any value other than 0 up to 255 indicates that loop detection is on and specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

The MPLS LDP threshold (mplsLdpFailedInitSessionThresholdExceeded) notification object provides a warning message that can be sent to an NMS 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 in Cisco IOS software and cannot be changed using either the command line interface (CLI) or an SNMP agent.

In general, 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 will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated.

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 to the existence of a condition in the network that may warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers or other vendor LSRs in an MPLS network. Among these incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI/VCI ranges (as noted) or nonoverlapping Frame Relay data-link connection identifier (DLCI) ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- Dissimilar LDP feature support

The **snmp-server enable traps mpls ldp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

If the **pv-limit** keyword is used, a message is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path-vector limits.

If the **session-down** keyword is used, a session-down message is generated when an LDP session between the router and its adjacent LDP peer is terminated.

If the **session-up** keyword is used, a message is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).

If the **threshold** keyword is used, a message is generated after eight failed attempts to establish an LDP session between the router and an LDP peer. The failures can be caused by any type of incompatibility between the devices.

All four keywords can be used in the same command in any combination.

Note An mplsLdpEntityFailedInitSessionThreshold trap is supported only on an LC-ATM.

Examples

In the following example, LDP-specific informs are enabled and will be sent to the host myhost.cisco.com through use of community string defined as public:

```
Router(config)# snmp-server enable traps mpls ldp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public mpls-ldp
```

Related Commands

Command	Description
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-server enable traps mpls rfc ldp

To enable the sending of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Simple Network Management Protocol (SNMP) notifications defined in RFC 3815, use the **snmp-server enable traps mpls rfc ldp** command in global configuration mode. To disable the sending of MPLS LDP notifications, use the **no** form of this command.

snmp-server enable traps mpls rfc ldp [**pv-limit** | **session-down** | **session-up** | **threshold**]

no snmp-server enable traps mpls rfc ldp [**pv-limit** | **session-down** | **session-up** | **threshold**]

Syntax Description

pv-limit	(Optional) Enables or disables MPLS RFC LDP path-vector (PV) limit mismatch notifications (mplsLdpPathVectorLimitMismatch).
session-down	(Optional) Enables or disables MPLS RFC LDP session down notifications (mplsLdpSessionDown).
session-up	(Optional) Enables or disables MPLS RFC LDP session up notifications (mplsLdpSessionUp).
threshold	(Optional) Enables or disables MPLS RFC LDP threshold exceeded notifications (mplsLdpInitSessionThresholdExceeded).

Command Default

The sending of SNMP notifications is disabled by default.
If you do not specify an optional keyword, all four types of MPLS RFC LDP notifications are enabled on the label switch router (LSR).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to enable the LDP notifications supported in *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP),* RFC 3815.

The MPLS LDP **pv-limit** (mplsLdpPathVectorLimitMismatch) notification provides a warning message that can be sent to the network management station (NMS) when two routers engaged in LDP operations have a dissimilar path vector limits. We recommend that all LDP-enabled routers in the network be configured with the same path vector limits.

The value of the path vector limit can range from 0 to 255; a value of 0 indicates that loop detection is off; any value other than 0 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.

The MPLS LDP **threshold** (mplsLdpFailedInitSessionThresholdExceeded) notification object provides a warning message that can be sent to an NMS 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 eight. This default value is implemented in Cisco IOS software and cannot be changed using either the command-line interface (CLI) or an SNMP agent.

In general, 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 Virtual Path Identifier (VPI) and Virtual Channel Identifier (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 will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated.

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 to the existence of a condition in the network that may warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers or between Cisco routers and other vendor LSRs in an MPLS network. Among these incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI and VCI ranges (as noted) or nonoverlapping Frame Relay Data Link Connection Identifier (DLCI) ranges between LSRs attempting to configure an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- Dissimilar LDP feature support

The **snmp-server enable traps mpls rfc ldp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

If the **pv-limit** keyword is used, a message is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.

If the **session-down** keyword is used, a session-down message is generated when an LDP session between the router and its adjacent LDP peer is terminated.

If the **session-up** keyword is used, a message is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).

If the **threshold** keyword is used, a message is generated after eight failed attempts to establish an LDP session between the router and an LDP peer. The failures can be caused by any type of incompatibility between the devices.

Examples

In the following example, LDP-specific informs are enabled and will be sent to the host myhost.cisco.com through use of community string defined as public:

```
Router(config)# snmp-server enable traps mpls rfc ldp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public mpls-ldp
```

Related Commands

Command	Description
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

snmp-server enable traps mpls rfc vpn

To enable the sending of Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Simple Network Management Protocol (SNMP) notifications defined in RFC 4382, use the **snmp-server enable traps mpls rfc vpn** command in global configuration mode. To disable the sending of MPLS VPN notifications, use the **no** form of this command

snmp-server enable traps mpls rfc vpn [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid threshold**] [**vrf-down**] [**vrf-up**]

no snmp-server enable traps mpls rfc vpn [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid threshold**] [**vrf-down**] [**vrf-up**]

Syntax Description

illegal-label	(Optional) Enables or disables an MPLS RFC VPN notification for any illegal labels received on a VPN routing and forwarding (VRF) instance interface.
max-thresh-cleared	(Optional) Enables or disables an MPLS RFC VPN notification when the number of routes attempts to exceed the maximum limit and then drops below the maximum number of routes.
max-threshold	(Optional) Enables or disables an MPLS RFC VPN notification when a route creation attempt was unsuccessful because the maximum route limit was reached.
mid-threshold	(Optional) Enables or disables an MPLS RFC VPN warning when the number of routes created has exceeded the warning threshold.
vrf-down	(Optional) Enables or disables an MPLS RFC VPN notification when the last interface associated with a VRF transitions to the down state.
vrf-up	(Optional) Enables or disables an MPLS RFC VPN notification when the first interface associated with a VRF transitions to the up state when previously all interfaces were in the down state.

Command Default

The sending of SNMP notifications is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If this command is used without any of the optional keywords, all MPLS RFC VPN notification types are enabled.

The **illegal-label** keyword enables a notification for illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have a Label Forwarding Information Base (LFIB) entry, or do not match table IDs for the label.

When the **max-thresh-cleared** keyword is used and you attempt to create a route on a VRF that already contains the maximum number of routes, the mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notification is sent (if enabled). When you remove routes from the VRF so that the number of routes falls below the set limit, the mplsL3VpnNumVrfRouteMaxThreshCleared notification is sent. You can clear all routes from the VRF by using the **clear ip route vrf** command.

The **max-threshold** keyword enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached. Another 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 **maximum routes** command in VRF configuration mode. If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the maximum threshold values. An mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notification is not sent until the second address family reaches its maximum route threshold. Routes are not added to the address family that has already reached its maximum route threshold.

Note If you configure a single address-family VRF with a maximum and middle threshold, and later add the other address-family configuration to your VRF without configuring a maximum threshold, you no longer receive a maximum threshold notification for the original address family when the threshold is reach, but routes would no longer be added to the routing table for this address family.

The warning that the **mid-threshold** keyword enables is sent only at the time the warning threshold is exceeded. If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the middle or warning threshold values. An mplsL3VpnVrfRouteMidThreshExceeded notification is not sent until the second address family reaches its warning threshold.

The values for the **mid-threshold** and **max-threshold** keywords are set using the **maximum routes** *limit* {*warn-threshold* | **warning-only**} VRF command in configuration mode.

The **maximum routes** command gives you two options in the VRF address family configuration mode:

- **maximum routes** *limit* **warning-only**—generates a warning message when you attempt to exceed the limit. The specified limit is not enforced.

  If you use the **maximum routes** *limit* **warning-only** command with the **snmp-server enable traps mpls rfc vpn** command, a mid-threshold SNMP notification is generated when the *limit* value is reached or exceeded. No max-threshold SNMP notification is generated.

- **maximum routes** *limit warn-threshold*—generates a warning message when the *warn-threshold* is reached. The specified limit is enforced.

  If you use the **maximum routes** *limit warn-threshold* command with the **snmp-server enable traps mpls rfc vpn** command, a mid-threshold SNMP notification is generated when the *warn-threshold* value is reached. A max-threshold notification is generated when the *limit* value is reached.

Note When both IPv4 and IPv6 address-family configurations exist, the MPLS-L3-VPN-STD-MIB displays the aggregate value of the maximum route settings (not to exceed the max int32 value). If the maximum route limit is configured for one address family and not for the other address family, the aggregate value is max int32 (4,294,967,295).

The notification types described are defined in the following MIB objects of the MPLS-L3-VPN-STD-MIB:

- mplsL3VpnVrfUp
- mplsL3VpnVrfDown
- mplsL3VpnVrfRouteMidThreshExceeded
- mplsL3VpnVrfNumVrfRouteMaxThreshExceeded
- mplsL3VpnNumVrfSecIllglLblThrshExcd
- mplsL3VpnNumVrfRouteMaxThreshCleared

Examples

In the following example, MPLS RFC VPN trap notifications are sent to the host specified as 172.31.156.34 using the community string named public if a VRF transitions from an up or down state:

```
Router(config)# snmp-server host 172.31.156.34 traps public mpls-vpn
Router(config)# snmp-server enable traps mpls rfc vpn vrf-down vrf-up
```

Related Commands

Command	Description
clear ip route vrf	Removes routes from the VRF routing table.
maximum routes	Limits the maximum number of routes in a VRF to prevent a PE router from importing too many routes.
snmp-server host	Specifies the recipient of SNMP notifications.

snmp-server enable traps mpls traffic-eng

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps mpls traffic-eng** command in global configuration mode. To disable MPLS traffic engineering tunnel state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls traffic-eng [**up** | **down** | **reroute**]

no snmp-server enable traps mpls traffic-eng [**up** | **down** | **reroute**]

Syntax Description

up	(Optional) Enables only mplsTunnelUp notifications { mplsTeNotifyPrefix 1 }.
down	(Optional) Enables only mplsTunnelDown notifications { mplsTeNotifyPrefix 2}.
reroute	(Optional) Enables or disables only mplsTunnelRerouted notifications {mplsTeNotifyPrefix 3}.

Command Default

SNMP notifications are disabled.

When this command is used without keywords, all available trap types (up, down, reroute) are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables MPLS traffic engineering tunnel notifications. MPLS tunnel state-change notifications, when enabled, will be sent when the connection moves from an “up” to “down” state, when a connection moves from a “down” to “up” state, or when a connection is rerouted. If you do not specify a keyword in conjunction with this command, all three types of MPLS traffic engineering tunnel notifications are sent.

When the **up** keyword is used, mplsTunnelUp notifications are sent to a network management system (NMS) when an MPLS traffic engineering tunnel is configured and the tunnel transitions from an operationally “down” state to an “up” state.

When the **down** keyword is used, mplsTunnelDown notifications are generated and sent to the NMS when an MPLS traffic engineering tunnel transitions from an operationally “up” state to a “down” state.

When the **reroute** keyword is used, mplsTunnelRerouted notifications are sent to the NMS under the following conditions:

- The signaling path of an existing MPLS traffic engineering tunnel fails and a new path option is signaled and placed into effect (that is, the tunnel is rerouted).
- The signaling path of an existing MPLS traffic engineering 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

The mplsTunnelReoptimized notification is not generated when an MPLS traffic engineering tunnel is reoptimized. However, an mplsTunnelReroute notification is generated. Thus, at the NMS, you cannot distinguish between a tunnel reoptimization and a tunnel reroute event.

The **snmp-server enable traps mpls traffic-eng** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send MPLS notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls traffic-eng
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps mpls vpn

To enable the router to send Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)-specific Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps mpls vpn** command in global configuration mode. To disable MPLS VPN specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls vpn [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid-threshold**] [**vrf-down**] [**vrf-up**]

no snmp-server enable traps mpls vpn [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid-threshold**] [**vrf-down**] [**vrf-up**]

Syntax Description

illegal-label	(Optional) Enables a notification for any illegal labels received on a VPN routing/forwarding instance (VRF) interface.
max-thresh-cleared	(Optional) Enables a notification when the number of routes attempts to exceed the maximum limit and then drops below the maximum number of routes.
max-threshold	(Optional) Enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached.
mid-threshold	(Optional) Enables a warning that the number of routes created has exceeded the warning threshold.
vrf-down	(Optional) Enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.
vrf-up	(Optional) Enables a notification for the assignment of a VRF to an interface that is operational or for the transition of a VRF interface to the operationally up state.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(30)S	This command was updated with the **max-thresh-cleared** keyword.
12.2(28)SB2	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is used without any of the optional keywords, all MPLS VPN notification types are enabled.

The **illegal-label** keyword enables a notification for illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have a Label Forwarding Information Base (LFIB) entry, or do not match table IDs for the label.

When the **max-thresh-cleared** keyword is used and 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.

The **max-threshold** keyword enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached. Another 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 **maximum routes** command in VRF configuration mode.

The warning that the **mid-threshold** keyword enables is sent only at the time the warning threshold is exceeded.

For the **vrf-up** (mplsVrfIfUp) or **vrf-down** (mplsVrfIfDown) notifications to be issued from an ATM or Frame Relay subinterface, you must first configure the **snmp-server traps atm subif** command or the **snmp-server traps frame-relay subif** command on the subinterfaces, respectively.

The values for the **mid-threshold** and **max-threshold** keywords are set using the **maximum routes** *limit* {*warn-threshold* | **warning-only**} VRF command in configuration mode.

The **maximum routes** command gives you two options:

- **maximum routes** *limit* **warning-only**—generates a warning message when you attempt to exceed the limit. The specified limit is not enforced.

  If you use the **maximum routes** *limit* **warning-only** command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification is generated when the *limit* value is reached or exceeded. No max-threshold SNMP notification is generated.

- **maximum routes** *limit warn-threshold*—generates a warning message when the *warn-threshold* is reached. The specified limit is enforced.

  If you use the **maximum routes** *limit warn-threshold* command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification is generated when the *warn-threshold* value is reached. A max-threshold notification is generated when the *limit* value is reached.

The notification types described are defined in the following MIB objects of the PPVPN-MPLS-VPN-MIB:

- mplsVrfIfUp
- mplsVrfIfDown
- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded

- mplsNumVrfSecIllegalLabelThreshExceeded

The cMplsNumVrfRouteMaxThreshCleared notification type is defined in the CISCO-IETF-PPVPN-MPLS-VPN-MIB.

Examples

In the following example, MPLS VPN trap notifications are sent to the host specified as 172.31.156.34 using the community string named public if a VRF transitions from an up or down state:

```
Router(config)# snmp-server host 172.31.156.34 traps public mpls-vpn
Router(config)# snmp-server enable traps mpls vpn vrf-down vrf-up
```

Related Commands

Command	Description
maximum routes	Sets the warning threshold and route maximum for VRFs.
snmp-server enable traps atm subif	Enables ATM subinterface SNMP notifications.
snmp-server enable traps frame-relay subif	Enables Frame Relay subinterface SNMP notifications.
snmp-server host	Specifies the recipient of SNMP notifications.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number* | *acl-name*]]

no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.

notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
[*acl-number* | *acl-name*]	(Optional) The *acl-number* argument is an integer from 1 to 99 that identifies a previously configured standard access list. The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.(3)T	This command was introduced.
12.0(23)S	The **context** *context-name* keyword and argument pair was added.
12.3(2)T	The **context** *context-name* keyword and argument pair was integrated into Cisco IOS Release 12.3(2)T, and support for standard named access lists (acl-name) was added.
12.0(27)S	The **ipv6** *named-access-list* keyword and argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The **ipv6** *named-access-list* keyword and argument pair was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

The *notify-view* option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user**—Configures an SNMP user.
2. **snmp-server group**—Configures an SNMP group, without adding a notify view.
3. **snmp-server host**—Autogenerates the notify view by specifying the recipient of a trap operation.

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.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Examples

Create an SNMP Group

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Router(config)# snmp-server group public v2c access lmnop
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Router(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Router(config)# snmp-server context A
Router(config)# snmp mib community commA
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

Related Commands

Command	Description
show snmp group	Displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.
snmp mib community-map	Associates a SNMP community with an SNMP context, engine ID, security name, or VPN target list.
snmp-server host	Specifies the recipient of a SNMP notification operation.
snmp-server user	Configures a new user to a SNMP group.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]} [*community-string* [**udp-port** *port*] [*notification-type*]]

no snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]} [*community-string* [**udp-port** *port*] [*notification-type*]]

Syntax Description

hostname	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
ip-address	IP address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications.
vrf-name	(Optional) VPN VRF instance used to send SNMP notifications.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
informs	(Optional) Specifies that notifications should be sent as informs.
version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. If you use the **version** keyword, one of the following keywords must be specified: • **1**—SNMPv1. • **2c**—SNMPv2C. • **3**—SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**. One of the following three optional security level keywords can follow the **3** keyword: – **auth**—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string is sent with the notification operation. **Note** You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command. **Note** The "at" sign (@) is used for delimiting the context information.

udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an NMS host.
port	(Optional) UDP port number of the NMS host. The default is 162.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of the following keywords: • **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. • **calltracker**—Sends Call Tracker call-start/call-end notifications. • **cef** — Sends notifications related to Cisco Express Forwarding. • **config**—Sends configuration change notifications. • **cpu**—Sends CPU-related notifications. • **director**—Sends notifications related to DistributedDirector. • **dspu**—Sends downstream physical unit (DSPU) notifications. • **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications. • **entity**—Sends Entity MIB modification notifications. • **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • **flash**—Sends flash media insertion and removal notifications. • **frame-relay**—Sends Frame Relay notifications. • **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications. • **iplocalpool**—Sends IP local pool notifications. • **ipmobile**—Sends Mobile IP notifications. • **ipsec**—Sends IP Security (IPsec) notifications. • **isdn**—Sends ISDN notifications. • **l2tun-pseudowire-status**—Sends pseudowire state change notifications. • **l2tun-session**—Sends Layer 2 tunneling session notifications. • **license**—Sends licensing notifications as traps or informs. • **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications. • **memory**—Sends memory pool and memory buffer pool notifications. • **mpls-ldp**—Sends Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.

- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **nhrp**—Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.

- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stun**—Sends serial tunnel (STUN) notifications.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **x25**—Sends X.25 event notifications.

Command Default This command is disabled by default. A recipient is not specified to receive notifications.

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	• The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature. • The **hsrp** notification-type keyword was added. • The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	• The **vrf** *vrf-name* keyword/argument combination was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	• The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	• The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
12.2(13)T	• The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	• The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
12.3(4)T	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf** notification-type keyword was added.
12.3(8)T	The **iplocalpool** notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The **vrrp** keyword was added.
12.3(14)T	• Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **eigrp** notification-type keyword was added.
12.4(20)T	The **license** notification-type keyword was added.
15.0(1)M	This command was modified. The **nhrp** notification-type keyword was added.
Cisco IOS Release 12.0S	
12.0(17)ST	The **mpls-traffic-eng** notification-type keyword was integrated into Cisco IOS Release 12.0(17)ST.
12.0(21)ST	The **mpls-ldp** notification-type keyword was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	• All features in the Cisco IOS Release 12.0ST train were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.

Release	Modification
12.0(23)S	The **l2tun-session** notification-type keyword was added.
12.0(26)S	The **memory** notification-type keyword was added.
12.0(27)S	• Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword argument pair was integrated into Cisco IOS Release 12.0(27)S to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The **l2tun-pseudowire-status** notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The **cef** notification-type keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Note If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with a SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter a **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a user so data is stored using the VPN.

Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the command-line interface (CLI) interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 162 maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 162 SNMP-server enable traps Commands and Corresponding Notification Keywords

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	**l2tun-session**
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng[1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**

1. See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 192.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

Note The "at" sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community@VLAN-ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 192.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to company.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host company.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 192.40.3.130 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP trap that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

status (pseudowire class)

To enable the router to send pseudowire status messages to a peer router, even when the attachment circuit is down, use the **status** command in pseudowire class configuration mode. To disable the pseudowire status messages, use the **no** form of this command.

status

no status

Syntax Description

This command has no arguments or keywords.

Command Default

Pseudowire status messages are sent and received if both routers support the messages.

Command Modes

Pseudowire class configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

Both peer routers must support the ability to send and receive pseudowire status messages in label advertisement and label notification messages. If both peer routers do not support pseudowire status messages, Cisco recommends that you disable the messages with the **no status** command.

Examples

The following example enables the router to send pseudowire status messages to a peer router:

```
enable
 configure terminal
 pseudowire-class test1
  status
  encapsulation mpls
```

Related Commands

Command	Description
debug mpls l2transport vc	Displays debug messages about pseudowire status.
show mpls l2transport vc detail	Displays pseudowire status messages.

status redundancy

To designate one pseudowire as the master or slave to display status information for both active and backup pseudowires, use the **status redundancy** command in pseudowire class configuration mode. To disable the pseudowire as the master or slave, use the **no** form of this command.

status redundancy {**master** | **slave**}

no status redundancy {**master** | **slave**}

Syntax Description

master	Designates one pseudowire to work as the master.
slave	Designates one pseudowire to work as the slave.

Command Default

The pseudowire is in slave mode.

Command Modes

Pseudowire-class configuration mode (config-pw)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.

Usage Guidelines

One pseudowire must be the master and the other must be assigned the slave. You cannot configure both pseudowires as master or slave.

Examples

The following example designates the pseudowire as the master:

```
Router(config-pw)# status redundancy master
```

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and pseudowires

switching tlv

To advertise the switching point type-length variable (TLV) in the label binding, use the **switching tlv** command in pseudowire class configuration mode. To disable the display of the TLV, use the **no** form of this command.

switching tlv

no switching tlv

Syntax Description

This command has no arguments or keywords.

Command Default

Switching point TLV data is advertised to peers.

Command Modes

Pseudowire class configuration (config-pw-class)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.

Usage Guidelines

The pseudowire switching point TLV information includes the following information:

- Pseudowire ID of the last pseudowire segment traversed
- Pseudowire switching point description
- Local IP address of the pseudowire switching point
- Remote IP address of the last pseudowire switching point that was crossed or the T-PE router

By default, switching point TLV data is advertised to peers.

Examples

The following example enables the display of the pseudowire switching TLV:

```
Router(config)# pseudowire-class atom
Router(config-pw-class)# switching tlv
```

Related Commands

Command	Description
show mpls l2transport binding	Displays switching point TLV information.
show mpls l2transport vc detail	Displays switching point TLV information.

ttag-control-protocol vsi

Note Effective with Cisco IOS Release 12.4(20)T, the **tag-control-protocol vsi** command is not available in Cisco IOS software.

To configure the use of Virtual Switch Interface (VSI) on a particular master control port, use the **tag-control-protocol vsi** command in interface configuration mode. To disable VSI, use the **no** form of this command.

tag-control-protocol vsi [**base-vc** *vpi vci*] [**delay** *seconds*] [**id** *controller-id*] [**keepalive** *timeout*] [**nak** [**basic** | **extended**]] [**retry** *timeout-count*] [**slaves** *slave-count*]

no tag-control-protocol vsi [**base-vc** *vpi vci*] [**delay** *seconds*] [**id** *controller-id*] [**keepalive** *timeout*] [**nak** [**basic** | **extended**]] [**retry** *timeout-count*] [**slaves** *slave-count*]

Syntax Description

base-vc *vpi vci*	(Optional) Determines the VPI/VCI value for the channel to the first slave. The default is 0/40. Together with the slave value, this value determines the VPI/VCI values for the channels to all of the slaves, which are as follows: • *vpi/vci* • *vpi/vci*+1, and so on • *vpi/vci*+*slave-count*-1
delay *seconds*	(Optional) Specifies the delay time to start a new VSI session after the system comes up or after you enter the command. If a VSI session is already running, the **delay** keyword has no effect for the current session. The delay is implemented when a new VSI session starts. The default is 0. The valid range of values is 0 to 300.
id *controller-id*	(Optional) Determines the value of the controller-id field present in the header of each VSI message. The default is 1.
keepalive *timeout*	(Optional) Determines the value of the keepalive timer (in seconds). Make sure that the keepalive timer value is greater than the value of the retry timer times the retry timer +1. The default is 15 seconds.

nak [**basic** | **extended**]	(Optional) Allows the label switch controller (LSC) to request extended negative acknowledgment (NAK) responses from the VSI slave. The extended NAK response indicates a dangling connection on the VSI slave. If the slave sends an extended NAK response code, the LSC sends a delete connection command that enables the VSI slave to delete the dangling connection. Use the **basic** keyword to specify the NAK 11 and NAK 12 response codes from the VSI. If you use the **nak basic** keywords, support for extended NAK is not enabled on the LSC. The interface configuration does not indicate that basic NAK support is enabled. The output of the **show controller vsi session** command does not indicate that basic NAK support is enabled. Use the **extended** keyword to specify extended NAK codes 51 - 54 from the VSI, which are supported in VSI protocol version 2.4. If you use the **nak extended** keywords, support for extended NAK is enabled on the LSC. The interface configuration indicates that extended NAK support is enabled. The output of the **show controller vsi session** command also indicates that extended NAK support is enabled. **Note** Use the **nak extended** keyword only if all VSI slaves support extended NAK codes.
retry *timeout-count*	(Optional) Determines the value of the message retry timer (in seconds) and the maximum number of retries. The default is 8 seconds and 10 retries.
slaves *slave-count*	(Optional) Determines the number of slaves reachable through this master control port. The default is 14 (suitable for the Cisco BPX switch).

Defaults

VSI is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(15)T	The **delay** keyword was added.
12.3(2)T	The **nak** keyword was added.
12.4(20)T	This command was removed.

Usage Guidelines

- The command is only available on interfaces that can serve as a VSI master control port. Cisco recommends that all options to the **tag-control-protocol vsi** command be entered at the same time.
- After VSI is active on the control interface (through the earlier issuance of a **tag-control-protocol vsi** command), reentering the command may cause all associated XTagATM interfaces to shut down and restart. In particular, if you reenter the **tag-control-protocol vsi** command with any of the following options, the VSI shuts down and reactivates on the control interface:
  - **id**
  - **base-vc**

- **slaves**

The VSI remains continuously active (that is, the VSI does not shut down and then reactivate) if you reenter the **tag-control-protocol vsi** command with only one or both of the following options:

- **keepalive**
- **retry**
- **delay**

In either case, if you reenter the **tag-control-protocol vsi** command, this causes the specified options to take on the newly specified values; the other options retain their previous values. To restore default values to all the options, enter the **no tag-control-protocol** command, followed by the **tag-control-protocol vsi** command.

Examples

The following example shows how to configure the VSI driver on the control interface:

```
Router(config)# interface atm 0/0
Router(config-if)# tag-control-protocol vsi base-vc 0 51
```

The following example enables extended NAK support:

```
Router(config-if)# tag-control-protocol vsi nak extended
```

The following example shows that extended NAK support is enabled, as shown by the bold output:

```
Router# show running-config interface atm0/0

Building configuration...
Current configuration : 113 bytes
interface ATM0/0
 no ip address
 shutdown
 label-control-protocol vsi nak extended
 no atm ilmi-keepalive
end
```

The **show controllers vsi session** command also indicates that extended NAK support is enabled, as shown by the bold output:

```
Router# show controllers vsi session

Interface    Session  VCD    VPI/VCI    Switch/Slave Ids   Session State
ATM0/0       0        1      0/40       0/0                UNKNOWN
ATM0/0       1        2      0/41       0/0                UNKNOWN
ATM0/0       2        3      0/42       0/0                UNKNOWN
ATM0/0       3        4      0/43       0/0                UNKNOWN
ATM0/0       4        5      0/44       0/0                UNKNOWN
ATM0/0       5        6      0/45       0/0                UNKNOWN
ATM0/0       6        7      0/46       0/0                UNKNOWN
ATM0/0       7        8      0/47       0/0                UNKNOWN
ATM0/0       8        9      0/48       0/0                UNKNOWN
ATM0/0       9        10     0/49       0/0                UNKNOWN
ATM0/0       10       11     0/50       0/0                UNKNOWN
ATM0/0       11       12     0/51       0/0                UNKNOWN
ATM0/0       12       13     0/52       0/0                UNKNOWN
ATM0/0       13       14     0/53       0/0                UNKNOWN
Extended NAK support is enabled on LSC
```

Table 163 describes the significant fields shown in the display.

Table 163 show controllers vsi session Field Descriptions

Field	Description
Interface	Control interface name.
Session	Session number (from 0 to <*n*–1>), where *n* is the number of sessions on the control interface.
VCD	Virtual circuit descriptor (virtual circuit number). Identifies the VC carrying the VSI protocol between the master and the slave for this session.
VPI/VCI	Virtual path identifier or virtual channel identifier (for the VC used for this session).
Switch/Slave Ids	Switch and slave identifiers supplied by the switch.
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. Other possible states include the following: • CONFIGURING • RESYNC-STARTING • RESYNC-UNDERWAY • RESYNC-ENDING • DISCOVERY • SHUTDOWN-STARTING • SHUTDOWN-ENDING • INACTIVE

trace mpls

To discover Multiprotocol Label Switching (MPLS) label switched path (LSP) routes that packets actually take when traveling to their destinations, use the **trace mpls** command in privileged EXEC mode.

trace mpls
{**ipv4** *destination-address/destination-mask-length*
| **traffic-eng Tunnel** *tunnel-number*
| **pseudowire** *destination-address vc-id* **segment** *segment-number* [*segment number*]}
[**timeout** *seconds*]
[**destination** *address-start* [*address-end* | *address-increment*]]
[**revision** {**1** | **2** | **3** | **4**}]
[**source** *source-address*]
[**exp** *exp-bits*]
[**ttl** *maximum-time-to-live*]
[**reply** {**dscp** *dscp-bits* | **mode** *reply-mode* {**ipv4** | **no-reply** | **router-alert**} | **pad-tlv**}]
[**force-explicit-null**]
[**output interface** *tx-interface* [**nexthop** *ip-address*]]
[**flags fec**]
[**revision** *tlv-revision-number*]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
destination-address	Address prefix of the target to be tested.
/destination-mask-length	Number of bits in the network mask of the target address. The slash is required.
traffic-eng Tunnel *tunnel-number*	Specifies the destination type as an MPLS traffic engineering (TE) tunnel.
pseudowire	Specifies the destination type as an Any Transport over MPLS (AToM) virtual circuit (VC).
ipv4-address	IPv4 address of the AToM VC to be tested.
vc-id	Specifies the VC identifier of the AToM VC to be tested.
segment	Specifies a segment of a multisegment pseudowire.
segment-number	A specific segment of the multisegment pseudowire or a range of segments, indicated by two segment numbers.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds. The range is from 0 to 3600. The default is 2 seconds.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) The beginning network 127 address.
address-end	(Optional) The ending network 127 address.
address-increment	(Optional) Number by which to increment the network 127 address.

revision {**1** | **2** | **3** | **4**}	(Optional) Selects the type, length, values (TLVs) version of the implementation. Use the **revision 4** default unless attempting to interoperate with devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2. If you do not select a **revision** keyword, the software uses the latest version. See Table 164 in the"Revision Keyword Usage" section of the "Usage Guidelines" section for information on when to select the **1**, **2**, **3**, and **4** keywords.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
ttl *maximum-time-to-live*	(Optional) Specifies a maximum hop count. Default is 30.
reply dscp *dscp-bits*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header ToS byte set to the value specified in the **reply dscp** keyword.
reply mode *reply-mode*	(Optional) Specifies the reply mode for the echo request packet. The *reply-mode* is one of the following: **ipv4**—Reply with an IPv4 User Datagram Protocol (UDP) packet (default). **no-reply**—Do not send an echo request packet in response. **router-alert**—Reply with an IPv4 UDP packet with router alert.
reply pad-tlv	(Optional) Tests the ability of the sender of an echo reply to support the copy pad TLV to echo reply.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
flags fec	(Optional) Requests that target Forwarding Equivalence Class (FEC) stack validation be done at the egress router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Be sure to use this keyword in conjunction with the **ttl** keyword.
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	The **reply dscp** and **reply pad-tlv** keywords were added.
12.4(6)T	The following keywords were added: **force-explicit-null**, **output interface**, **flags fec**, and **revision**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **nexthop** keyword was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3	The **segment** keyword was added.
12.2(33)SRE	This command was modified. Restrictions were added to the **pseudowire** keyword.

Usage Guidelines

Use the **trace mpls** command to validate, test, or troubleshoot IPv4 LDP LSPs and IPv4 Resource Reservation Protocol (RSVP) TE tunnels.

UDP Destination Address Usage

The destination address is a valid 127/8 address. You can specify a single address or a range of numbers from 0.0.0 to *x.y.z*, where *x*, *y*, and *z* are numbers from 0 to 255 and correspond to the 127.*x.y.z* destination address.

The MPLS echo request destination address in the UDP packet is not used to forward the MPLS packet to the destination router. The label stack that is used to forward the echo request routes the MPLS packet to the destination router. The 127/8 address guarantees that the packets are routed to the localhost (the default loopback address of the router processing the address) if the UDP packet destination address is used for forwarding.

In addition, the destination address is used to adjust load balancing when the destination address of the IP payload is used for load balancing.

Time-to-Live Keyword Usage

The time-to-live value indicates the maximum number of hops a packet should take to reach its destination. The value in the TTL field in a packet is decremented by 1 each time the packet travels through a router.

For MPLS LSP ping, the TTL is a value after which the packet is discarded and an MPLS echo reply is sent back to the originating router.

For MPLS Multipath LSP Traceroute, the TTL is a maximum time-to-live value and is used to discover the number of downstream hops to the destination router. MPLS LSP Traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4, ...) to accomplish this.

Pseudowire Usage

The following keywords are not available with the **trace mpls pseudowire** command:

- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

Revision Keyword Usage

The **revision** keyword allows you to issue a **trace mpls ipv4** or **trace mpls traffic-eng** command based on the format of the TLV. Table 164 lists the revision option and usage guidelines for each option.

Table 164 Revision Options and Option Usage Guidelines

Revision Option	Option Usage Guidelines
1[1]	Not supported in Cisco IOS Release 12.4(11)T or later releases. Version 1 (draft-ietf-mpls-ping-03) For a device running Cisco IOS Release 12.0(27)S3 or a later release, you must use the **revision 1** keyword when you send LSP ping or LSP traceroute commands to devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2.
2	Version 2 functionality was replaced by Version 3 functionality before any images were shipped.
3	Version 3 (draft-ietf-mpls-ping-03). • For a device implementing Version 3 (Cisco IOS Release 12.0(27)S3 or a later release), you must use the **revision 1** keyword when you send the LSP **ping** or LSP **traceroute** command to a device implementing Version 1 (that is, either Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2). • A **ping mpls pseudowire** command does not work with devices running Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2.
4	• Version 8 (draft-ietf-mpls-ping-08)—Applicable before Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in Version 8. • RFC 4379 compliant—Applicable after Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in RFC 4379. This is the recommended version.

1. If you do not specify the **revision** keyword, the software uses the latest version.

Examples

The following example shows how to trace packets through an MPLS LDP LSP:

```
Router# trace mpls ipv4 10.131.191.252/32
```

Alternatively, you can use the interactive mode:

```
Protocol [ip]: mpls
Target IPv4, pseudowire or traffic-eng [ipv4]: <ipv4 |pseudowire |tunnel> ipv4
Target IPv4 address: 10.131.191.252
Target mask: /32
```

```
Repeat [1]:
Packet size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Destination start address:
Destination end address:
Source address:
EXP bits in mpls header [0]:
TimeToLive [255]:
Reply mode (2-ipv4 via udp, 3-ipv4 via udp with router alert) [2]:
Reply ip header DSCP bits [0]:

Tracing MPLS Label Switched Path to 10.131.191.252/32, timeout is 2 seconds

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0


Type escape sequence to abort.

  0 10.131.159.245 mtu 1500 []
! 1 10.131.191.252 100 ms
```

The following example shows how to trace packets through an MPLS TE tunnel:

```
Router# trace mpls traffic-eng Tunnel 0

Tracing MPLS TE Label Switched Path on Tunnel0, timeout is 2 seconds

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.131.159.230 mtu 1500 [Labels: 22 Exp: 0]
R 1 10.131.159.225 mtu 1500 [Labels: 22 Exp: 6] 72 ms
R 2 10.131.191.229 mtu 1504 [implicit-null] 72 ms
! 3 10.131.191.252 92 ms
```

Alternatively, you can use the interactive mode:

```
Router# traceroute
Protocol [ip]: mpls
Target IPv4 or tunnel [ipv4]: traffic-eng
Tunnel number [0]:
Repeat [1]:
Timeout in seconds [2]:
Extended commands? [no]:
Tracing MPLS TE Label Switched Path on Tunnel0, timeout is 2 seconds

Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
```

```
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.131.159.230 mtu 1500 [Labels: 22 Exp: 0]
R 1 10.131.159.225 mtu 1500 [Labels: 22 Exp: 6] 72 ms
R 2 10.131.191.229 mtu 1504 [implicit-null] 72 ms
! 3 10.131.191.252 92 ms
```

Use the **show running-config** command to verify the configuration of Tunnel 0 (shown in bold). The tunnel destination has the same IP address as the one in the earlier trace IPv4 example, but the trace takes a different path, even though tunnel 0 is not configured to forward traffic by means of autoroute or static routing. The **trace mpls traffic-eng** command is powerful; it enables you to test the tunnels to verify that they work before you map traffic onto them.

```
Router# show running-config interface tunnel 0

Building configuration...

Current configuration : 210 bytes
!
interface Tunnel0
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.131.191.252       <---- Tunnel destination IP address.
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng path-option 5 explicit name as1pe-long-path
end

Router# show mpls traffic-eng tunnels tunnel 0 brief

Signalling Summary:
    LSP Tunnels Process:            running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 1369 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    disabled
TUNNEL NAME               DESTINATION      UP IF     DOWN IF   STATE/PROT
PE_t0                     10.131.191.252   -         Et0/0     up/up

Router# show ip cef 10.131.191.252

10.131.191.252/32, version 37, epoch 0, cached adjacency 10.131.159.246
0 packets, 0 bytes
  tag information set, all rewrites owned
    local tag: 21
  via 10.131.159.246, Ethernet1/0, 0 dependencies
    next hop 10.131.159.246, Ethernet1/0
    valid cached adjacency
    tag rewrite with Et1/0, 10.131.159.246, tags imposed {}
```

The following example performs a trace operation on a multisegment pseudowire. The trace operation goes to segment 2 of the multisegment pseudowire.

```
Router# trace mpls pseudowire 10.10.10.9 220 segment 2

Tracing MS-PW segments within range [1-2] peer address 10.10.10.9 and timeout 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
```

```
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
L 1 10.10.9.9 4 ms [Labels: 18 Exp: 0]
    local 10.10.10.22 remote 10.10.10.9 vc id 220

! 2 10.10.3.3 4 ms [Labels: 16 Exp: 0]
    local 10.10.10.9 remote 10.10.10.3 vc id 220
```

Related Commands

Command	Description
ping mpls	Checks MPLS LSP connectivity.

trace mpls multipath

To discover all Multiprotocol Label Switching (MPLS) label switched paths (LSPs) from an egress router to an ingress router, use the **trace mpls multipath** command in privileged EXEC mode.

trace mpls multipath ipv4 *destination-address/destination-mask-length*
[**timeout** *seconds*]
[**interval** *milliseconds*]
[**destination** *address-start address-end*]
[**source** *source-address*]
[**exp** *exp-bits*]
[**ttl** *maximum-time-to-live*]
[**reply mode** {**ipv4** | **router-alert**}]
[**reply dscp** *dscp-value*]
[**retry-count** *retry-count-value*]
[**force-explicit-null**]
[**output interface** *tx-interface* [**nexthop** *ip-address*]]
[**hashkey ipv4 bitmap** *bitmap-size*]
[**flags fec**]
[**verbose**]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
destination-address	Address prefix of the target to be tested.
/destination-mask-length	Number of bits in the network mask of the target address. The slash is required.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds. The range is from 0 to 3600. The default is 2 seconds.
interval *milliseconds*	(Optional) Sets the time between successive MPLS echo requests in milliseconds. This allows you to pace the transmission of packets so that the receiving router does not drop packets. The default is 0 milliseconds. Valid values are from 0 to 3500000 milliseconds.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) The beginning network 127 address.
address-end	(Optional) The ending network 127 address.
source	(Optional) Specifies the source address or name.
source-address	(Optional) Source address or name.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
ttl *maximum-time-to-live*	(Optional) Specifies a maximum hop count.
reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. The reply mode is one of the following: • **ipv4** = Reply with an IPv4 User Datagram Protocol (UDP) packet (default). • **router-alert** = Reply with an IPv4 UDP packet with router alert.

reply dscp *dscp-value*	(Optional) Controls the differentiated services codepoint (DSCP) value of an echo reply. Allows the support of a class of service (CoS) in an echo reply.
retry-count *retry-count-value*	(Optional) Sets the number of timeout retry attempts during a multipath LSP trace. A retry is attempted if an outstanding echo request times out waiting for the corresponding echo reply. A *retry-count-value* of 0 means infinite retries. Valid values are from 0 to 10.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for MPLS echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next hop address.
hashkey ipv4 bitmap *bitmap-size*	(Optional) Allows you to control the hash key and multipath settings. • **ipv4**—Indicates an IPv4 address, which is the only hashkey type valid for multipath (type 8). • **bitmap** *bitmap-size*—Size of the bitmap IPv4 addresses.
flags fec	(Optional) Requests that target Forwarding Equivalence Class (FEC) stack validation of a transit router be done at the egress router. **Note** Be sure to use the **flags fec** keywords in conjunction with the **ttl** keyword.
verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.

Command Default

timeout = 2 seconds
interval = 0 milliseconds
reply mode = IPv4 via UDP (2)
Maximum time-to-live = 30 hops
Experimental bits in MPLS header = 0

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **trace mpls multipath** command to discover all possible paths between an egress and ingress router in multivendor networks that use IPv4 load balancing at the transit routers.

Use the **destination** *address-start address-end* keyword and arguments to specify a valid 127/8 address. You have the option to specify a single *x.y.z-address* or a range of numbers from 0.0.0 to *x.y.z*, where *x*, *y*, and *z* are numbers from 0 to 255 and correspond to the 127.*x.y.z* destination address. The MPLS echo

request destination address in the UDP packet is not used to forward the MPLS packet to the destination router. The label stack that is used to forward the echo request routes the MPLS packet to the destination router. The 127/8 address guarantees that the packets are routed to the localhost (the default loopback address of the router processing the address) if the UDP packet destination address is used for forwarding. In addition, the destination address is used to adjust load balancing when the destination address of the IP payload is used for load balancing.

Examples

The following example shows how to discover all IPv4 LSPs to a router whose IP address is 10.1.1.150:

```
Router# trace mpls multipath ipv4 10.1.1.150/32

Starting LSP Multipath Traceroute for 10.1.1.150/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
LLLL!
Path 0 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.0 LLL!
Path 1 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.1 L!
Path 2 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.5 LL!
Path 3 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
Paths (found/broken/unexplored) (4/0/0)
  Echo Request (sent/fail) (14/0)
  Echo Reply (received/timeout) (14/0)
  Total Time Elapsed 472 ms
```

The following example shows how to set the number of timeout retry attempts to 4 during a multipath LSP trace:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 retry-count 4

Starting LSP Multipath Traceroute for 10.1.1.150/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
LLLL!
Path 0 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.0 LLL!
Path 1 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.1 L!
Path 2 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.5 LL!
Path 3 found,
 output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
```

```
Paths (found/broken/unexplored) (4/0/0)
 Echo Request (sent/fail) (14/0)
 Echo Reply (received/timeout) (14/0)
 Total Time Elapsed 460 ms
```

The following example shows that outgoing MPLS Operation, Administration, and Management (OAM) echo request packets will go through the interface e0/0 and will be restricted to the path with the next hop address of 10.0.0.3:

```
Router# trace multipath ipv4 10.4.4.4/32 output interface e0/0 nexthop 10.0.0.3

Starting LSP Multipath Traceroute for 10.4.4.4/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
L!
Path 0 found,
 output interface Et0/0 nexthop 10.0.0.3
 source 10.0.0.1 destination 127.0.0.0

Paths (found/broken/unexplored) (1/0/0)
 Echo Request (sent/fail) (2/0)
 Echo Reply (received/timeout) (2/0)
 Total Time Elapsed 728 ms
```

Related Commands

Command	Description
echo	Customizes the default behavior of echo packets.
mpls oam	Enters MPLS OAM configuration mode for customizing the default behavior of echo packet.
ping mpls	Checks MPLS LSP connectivity.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

traffic-engineering filter

To specify a filter with the given number and properties, use the **traffic-engineering filter** command in router configuration mode. To disable this function, use the **no** form of this command.

traffic-engineering filter *filter-number* **egress** *ip-address mask*

no traffic-engineering filter

Syntax Description

filter-number	A decimal value representing the number of the filter.
egress *ip-address mask*	IP address and mask for the egress port.

Defaults

Disabled

Command Modes

Router configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must specify that the egress is the indicated address or mask, where egress is either the destination or the Border Gateway Protocol (BGP) next hop.

Examples

The following example shows how to configure a traffic engineering filter and a traffic engineering route for that filter over a label switched path (LSP)-encapsulated tunnel for the traffic engineering routing process:

```
Router(config)# router traffic-engineering
Router(config-router)# traffic-engineering filter 5 egress 10.0.0.1 255.255.255.255
Router(config-router)# traffic-engineering route 5 tunnel 5
```

Related Commands

Command	Description
show ip traffic-engineering routes	Displays information about the requested filters configured for traffic engineering.
traffic-engineering route	Configures a route for a specified filter, through a specified tunnel.

traffic-engineering route

To configure a route for a specified filter through a specified tunnel, use the **traffic-engineering route** command in router configuration mode. To disable this function, use the **no** form of this command.

traffic-engineering route *filter-number interface* [**preference** *number*] [**loop-prevention** {**on** | **off**}]

no traffic-engineering route *filter-number interface* [**preference** *number*] [**loop-prevention** {**on** | **off**}]

Syntax Description

filter-number	The number of the traffic engineering filter to be forwarded through the use of this traffic engineering route, if the route is installed.
interface	Label switched path (LSP)-encapsulated tunnel on which the traffic-passing filter should be sent, if this traffic engineering route is installed.
preference *number*	(Optional) This is a number from 1 to 255, with a lower value being more desirable. The default is 1.
loop-prevention	(Optional) A setting of **on** or **off**. The default is **on**.

Defaults

preference: 1
loop-prevention: on

Command Modes

Router configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The traffic engineering process is used to decide if a configured traffic engineering route should be installed in the forwarding table.

The first step is to determine if the route is up. If the route is enabled, the LSP tunnel interface is up, the loop prevention check is either disabled or passed, and the traffic engineering route is up.

If multiple routes for the same filter are up, a route is selected based on administrative preference.

If loop prevention is enabled, metrics are solicited from the tunnel tail, and the loop prevention algorithm is run on the result. For a discussion of the loop prevention algorithm, see the **show ip traffic-engineering metrics** command.

Examples

The following example shows how to configure a traffic engineering filter and a traffic engineering route for that filter through an LSP-encapsulated tunnel for the traffic engineering routing process:

```
Router(config)# router traffic-engineering
Router(config-router)# traffic-engineering filter 5 egress 10.0.0.1 255.255.255.255
Router(config-router)# traffic-engineering route 5 tunnel 5
```

Related Commands

Command	Description
show ip traffic-engineering configuration	Displays information about configured traffic engineering filters and routes.
show ip traffic-engineering routes	Displays information about the requested filters configured for traffic engineering.

tunnel destination access-list

To specify the access list that the template interface uses for obtaining the mesh tunnel interface destination address, use the **tunnel destination access-list** command in interface configuration mode. To remove the access list from this template interface, use the **no** form of this command.

tunnel destination access-list *num*

no tunnel destination access-list *num*

Syntax Description

num	Number of the access list.

Command Default

No default behavior or values to specify access lists.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command can be used only on template interfaces.

If you specify an access list that does not exist, no tunnels are set up. You need an access list to set up the destination addresses for the mesh tunnel interfaces.

If you enter the **shutdown** command on the autotemplate interface, the command is executed on all the cloned tunnel interfaces. To delete all the cloned tunnel interfaces, enter the **no tunnel destination** command on the autotemplate. To delete tunnel interfaces for a particular autotemplate, go to the particular interface and enter the **no tunnel destination** command.

Examples

The following example shows how to configure the template interface to use access-list 1 to obtain the tunnel destination address:

```
Router(config)# interface auto-template 1
Router(config-if)# tunnel destination access-list 1
```

Related Commands

Command	Description
interface auto-template	Creates the template interface.
mpls traffic-eng auto-tunnel mesh tunnel-num	Configures a range of mesh tunnel interface numbers.

tunnel destination list mpls traffic-eng

To specify a list of Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) destinations, use the **tunnel destination list mpls traffic-eng** command in interface configuration mode. To remove the destination list, use the **no** form of this command.

tunnel destination list mpls traffic-eng {**id** *destination-list-number* | **name** *destination-list-name*}

no tunnel destination list mpls traffic-eng {**id** *dest-list-number* | **name** *dest-list-name*}

Syntax Description

id *destination-list-identifier*	Specifies the number of a destination list. Valid range of numbers is 1–65535.
name *destination-list-name*	Specifies the name of a destination list.

Command Default

No destination list is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **tunnel destination list mpls traffic-eng** command to specify a list point-to-multipoint tunnels.

Examples

The following example configures point-to-multipoint traffic engineering on tunnel interface 1:

```
Router# interface tunnel1
Router(config-if)# tunnel mode mpls traffic-eng point-to-multipoint
Router(config-if)# tunnel destination list mpls traffic-eng name P2MP-DYN-DST-LIST
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays MPLS TE tunnels.
tunnel destination list mpls traffic-eng	Specifies the list of MPLS TE P2MP destinations.

tunnel destination mesh-group

To specify a mesh group that an autotemplate interface uses to signal tunnels for all mesh group members, use the **tunnel destination mesh group** command in interface configuration mode. To remove a mesh group from the template, use the **no** form of this command.

tunnel destination mesh-group *mesh-group-id*

no tunnel destination mesh-group *mesh-group-id*

Syntax Description

mesh-group-id	Number that identifies a specific mesh group.

Command Default

Mesh-groups are not advertised.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to associate a specific mesh group with an autotemplate. When a mesh group is associated with an autotemplate, the template interface signals tunnels for all mesh group members.

Examples

The following example shows how to configure an autotemplate to signal tunnels for mesh group 10:

```
Router(config)# interface auto-template 1
Router(config-if)# tunnel destination mesh-group 10
```

Related Commands

Command	Description
mpls traffic-eng mesh-group	Configures an IGP to allow MPLS TE LSRs that belong to the same mesh group to signal tunnels to the local router.

tunnel flow egress-records

To create a NetFlow record for packets that are encapsulated by a generic routing encapsulation (GRE) tunnel when both NetFlow and Cisco Express Forwarding are enabled, use the **tunnel flow egress-records** command in interface configuration mode. To disable NetFlow record creation, use the **no** form of this command.

tunnel flow egress-records

no tunnel flow egress-records

Syntax Description

This command has no arguments or keywords.

Defaults

A NetFlow record for encapsulated packets is not created.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When this command is enabled on a GRE tunnel with both Cisco Express Forwarding and NetFlow enabled, a NetFlow record is created for packets that are encapsulated by the tunnel.

Examples

The following example shows how to enable NetFlow record creation:

```
Router(config-if)# tunnel flow egress-records
```

Related Commands

Command	Description
show ip cache flow	Displays NetFlow switching statistics.

tunnel mode mpls traffic-eng

To set the mode of a tunnel to Multiprotocol Label Switching (MPLS) for traffic engineering, use the **tunnel mode mpls traffic-eng** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mode mpls traffic-eng

no tunnel mode mpls traffic-eng

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command specifies that the tunnel interface is for an MPLS traffic engineering tunnel and enables the various tunnel MPLS configuration options.

Examples

The following example shows how to set the mode of the tunnel to MPLS traffic engineering:

```
Router(config-if)# tunnel mode mpls traffic-eng
```

Related Commands

Command	Description
tunnel mpls traffic-eng affinity	Configures an affinity for an MPLS traffic engineering tunnel.
tunnel mpls traffic-eng autoroute announce	Instructs the IGP to use the tunnel in its enhanced SPF algorithm calculation (if the tunnel is up).
tunnel mpls traffic-eng bandwidth	Configures the bandwidth required for an MPLS traffic engineering tunnel.

Command	Description
tunnel mpls traffic-eng path-option	Configures a path option.
tunnel mpls traffic-eng priority	Configures setup and reservation priority for an MPLS traffic engineering tunnel.

tunnel mode mpls traffic-eng point-to-multipoint

To enable the configuration of a Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) tunnel, use the **tunnel mode mpls traffic-eng point-to-multipoint** command in interface configuration mode. To remove the tunnel, use the **no** form of this command.

tunnel mode mpls traffic-eng point-to-multipoint

no tunnel mode

Syntax Description

This command has no arguments or keywords.

Command Default

No point-to-multipoint tunnel mode is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the command to differentiate point-to-multipoint tunnels from point-to-point tunnels.

Examples

The following example configures point-to-multipoint traffic engineering on tunnel interface 1:

```
Router# interface Tunnel1
Router(config-if)# tunnel mode mpls traffic-eng point-to-multipoint
Router(config-if)# tunnel destination list mpls traffic-eng name P2MP-DYN-DST-LIST
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays MPLS TE tunnels.
tunnel destination list mpls traffic-eng	Specifies the list of MPLS TE P2MP destinations.

tunnel mpls traffic-eng affinity

To configure an affinity (the properties the tunnel requires in its links) for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng affinity** command in interface configuration mode. To disable the MPLS traffic engineering tunnel affinity, use the **no** form of this command.

tunnel mpls traffic-eng affinity *properties* [**mask** *mask value*]

no tunnel mpls traffic-eng affinity *properties* [**mask** *mask value*]

Syntax Description

properties	Attribute values required for links carrying this tunnel. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
mask *mask value*	(Optional) Link attribute to be checked. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

Defaults

properties: 0X00000000
mask value: 0X0000FFFF

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The affinity determines the attributes of the links that this tunnel will use (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of a link and the required affinity of the tunnel for that bit must match.

A tunnel can use a link if the tunnel affinity equals the link attributes and the tunnel affinity mask.

Any properties set to 1 in the affinity should also be 1 in the mask. In other words, affinity and mask should be set as follows:

```
tunnel_affinity = (tunnel_affinity and tunnel_affinity_mask)
```

Examples

The following example shows how to set the affinity of the tunnel to 0x0101 mask 0x303:

```
Router(config-if)# tunnel mpls traffic-eng affinity 0x0101 mask 0x303
```

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Sets the attributes for the interface.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute destination

To automatically route traffic through a traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng autoroute destination** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng autoroute destination

no tunnel mpls traffic-eng autoroute destination

Syntax Description

This command has no arguments or keywords.

Command Default

If you do not enter this command, manually-configured static routes are required.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **tunnel mpls traffic-eng autoroute destination** command prevents you from having to manually configure static routes. Use the **tunnel mpls traffic-eng autoroute destination** command because interarea TE tunnels cross areas.

For interarea tunnels, the **tunnel mpls traffic-eng autoroute announce** command and the **tunnel mpls traffic-eng forwarding-adjacency** command are not operational.

Examples

The following example specifies that tunnel 103 has autoroute destination enabled:

```
Router(config)# interface Tunnel103
Router(config-if)# ip unnumbered Loopback0
Router(config-if)# tunnel destination 10.1.0.3
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng autoroute destination
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name 111-103
```

Related Commands

Command	Description
tunnel mpls traffic-eng autoroute announce	Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced SPF calculation.
tunnel mpls traffic-eng forwarding-adjacency	Advertises a TE tunnel as a link in an IGP network.

tunnel mpls traffic-eng auto-bw

To configure a tunnel for automatic bandwidth adjustment and to control the manner in which the bandwidth for a tunnel is adjusted, use the **tunnel mpls traffic-eng auto-bw** command in interface configuration mode. To disable automatic bandwidth adjustment for a tunnel, use the **no** form of this command.

tunnel mpls traffic-eng auto-bw [**collect-bw**] [**frequency** *seconds*] [**max-bw** *number*] [**min-bw** *number*]

no tunnel mpls traffic-eng auto-bw

Syntax Description

collect-bw	(Optional) Collects output rate information for the tunnel, but does not adjust the tunnel's bandwidth.
frequency *seconds*	(Optional) The interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds. Do not specify a value lower than the output rate sampling interval specified in the **mpls traffic-eng auto-bw** command.
max-bw *number*	(Optional) Maximum automatic bandwidth, in kbps, for this tunnel. The value is from 0 to 4294967295.
min-bw *number*	(Optional) Minimum automatic bandwidth, in kbps, for this tunnel. The value is from 0 to 4294967295. For information about the default, see "Usage Guidelines."

Command Default

You cannot control the manner in which the bandwidth for a tunnel is adjusted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you enter the command with no optional keywords or arguments, automatic bandwidth adjustment for the tunnel is enabled, with adjustments made every 24 hours and with no constraints on the bandwidth adjustment made.

To sample the bandwidth used by a tunnel without automatically adjusting it, specify the **collect-bw** keyword in the **tunnel mpls traffic-eng auto-bw** command.

If you do not specify the **collect-bw** keyword, the tunnel's bandwidth is adjusted to the largest average output rate sampled for the tunnel since the last bandwidth adjustment for the tunnel was made. If you do not specify the **collect-bw** keyword but you do enter some but not all of the other keywords, the defaults for the options not entered are: **frequency**, every 24hours; **min-bw**, unconstrained (0); and **max-bw**, unconstrained.

To constrain the bandwidth adjustment that can be made to a tunnel, use the **max-bw** or **min-bw** keyword and specify the permitted maximum allowable bandwidth or minimum allowable bandwidth, respectively.

The following rules apply to adjusting bandwidth on a tunnel:

- If the current bandwidth is less than 50 kbps, you can change the bandwidth only if the changed bandwidth is 10 kbps or more.
- If the current bandwidth is more than 50 kbps, you can change the bandwidth regardless of what percent it is of the current bandwidth.
- If the minimum or maximum bandwidth values are configured for a tunnel, the bandwidth stays between those values.
- If you configure a tunnel's bandwidth (in the **tunnel mpls traffic-eng bandwidth** command) and the minimum amount of automatic bandwidth (in the **tunnel mpls traffic-eng auto-bw** command), the minimum amount of automatic bandwidth adjustment is the lower of those two configured values. The default value of the **tunnel mpls traffic-eng bandwidth** command is 0.

The **no** form of the **tunnel mpls traffic-eng auto-bw** command disables bandwidth adjustment for the tunnel and restores the configured bandwidth for the tunnel bandwidth 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.

Note When you save the router configuration, the current bandwidth (not the originally configured bandwidth) is saved for tunnels with automatic bandwidth enabled.

Note Each **tunnel mpls traffic-eng auto-bw** command supersedes the previous one. Therefore, if you want to specify multiple arguments for a tunnel, you must specify them all in a single **tunnel mpls traffic-eng auto-bw** command.

Note Keywords for the **tunnel mpls traffic-eng auto-bw** command are order-dependent; you must enter them in the order in which they are listed in the command format.

Examples

The following example shows how to enable automatic bandwidth adjustment for tunnel102 and specify that the adjustments are to occur every hour:

```
Router(config)# interface tunnel102
Router(config-if)# tunnel mpls traffic-eng auto-bw frequency 3600
```

Related Commands

Command	Description
mpls traffic-eng auto-bw timers	Enables automatic bandwidth adjustment on a platform for tunnels configured for bandwidth adjustment.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.
tunnel mpls traffic-eng bandwidth	Configures bandwidth required for an MPLS traffic engineering tunnel,

tunnel mpls traffic-eng autoroute announce

To specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **tunnel mpls traffic-eng autoroute announce** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng autoroute announce

no tunnel mpls traffic-eng autoroute announce

Syntax Description

This command has no arguments or keywords.

Defaults

The IGP does not use the tunnel in its enhanced SPF calculation.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The only way to forward traffic onto a tunnel is by enabling this feature or by explicitly configuring forwarding (for example, with an interface static route).

Examples

The following example shows how to specify that the IGP should use the tunnel in its enhanced SPF calculation if the tunnel is up:

```
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

The following example shows how to specify that if the IGP is using this tunnel in its enhanced SPF calculation, the IGP should give it an absolute metric of 10:

```
Router(config-if)# tunnel mpls traffic-eng autoroute announce metric absolute 10
```

Related Commands

Command	Description
ip route	Establishes static routes.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute metric

To specify the Multiprotocol Label Switching (MPLS) traffic engineering tunnel metric that the Interior Gateway Protocol (IGP) enhanced shortest path first (SPF) calculation uses, use the **tunnel mpls traffic-eng autoroute metric** command in interface configuration mode. To disable the specified MPLS traffic engineering tunnel metric, use the **no** form of this command.

tunnel mpls traffic-eng autoroute metric {**absolute** | **relative**} *value*

no tunnel mpls traffic-eng autoroute metric

Syntax Description

absolute	Absolute metric mode; you can enter a positive metric value.
relative	Relative metric mode; you can enter a positive, negative, or zero value.
value	The metric that the IGP enhanced SPF calculation uses. The **relative** value can be from –10 to 10. **Note** Even though the value for a relative metric can be from –10 to 10, configuring a tunnel metric with a negative value is considered a misconfiguration. If from the routing table the metric to the tunnel tail appears to be 4, then the cost to the tunnel tail router is actually 3 because 1 is added to the cost for getting to the loopback address. In this instance, the lowest value that you can configure for the relative metric is –3.

Defaults

The default is metric relative 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to specify the use of MPLS traffic engineering tunnel metric negative 1 for the IGP enhanced SPF calculation:

```
Router(config-if)# tunnel mpls traffic-eng autoroute metric relative -1
```

Related Commands

Command	Description
show mpls traffic-eng autoroute	Displays the tunnels announced to IGP, including interface, destination, and bandwidth.
tunnel mpls traffic-eng autoroute announce	Instructs the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.

tunnel mpls traffic-eng backup-bw

To specify what types of label-switched paths (LSPs) can use a backup tunnel or whether the backup tunnel should provide bandwidth protection, and if so, how much, use the **tunnel mpls traffic-eng backup-bw** command in interface configuration mode.

tunnel mpls traffic-eng backup-bw {*kbps* | [**sub-pool** {*kbps* | **Unlimited**}] [**global-pool** {*kbps* | **Unlimited**}]} {*kbps* | [**class-type** {*kbps* | **Unlimited**}]

Syntax Description

kbps	Amount of bandwidth in kilobits per second (kbps), that this backup tunnel can protect. The router limits the number of LSPs that can use this backup tunnel so that the sum of the bandwidth of the LSPs does not exceed the specified amount of bandwidth. If there are multiple backup tunnels, the router will use the best-fit algorithm.
sub-pool	Only LSPs using bandwidth from the subpool can use the backup tunnel.
global-pool	Only LSPs using bandwidth from the global pool can use the backup tunnel.
class-type	Enter the class type.
Unlimited	Backup tunnel does not provide bandwidth protection. Any number of LSPs can use the backup tunnel, regardless of their bandwidth.

Command Default

If neither the **sub-pool** nor **global-pool** keyword is entered, any LSP (those using bandwidth from the subpool or global pool) can use this backup tunnel.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If both the **sub-pool** and **global-pool** keywords are specified, **sub-pool** keyword must be specified first on the command line. For example, **tunnel mpls traffic-eng backup-bw sub-pool 100 global-pool Unlimited** is legal, but it is not legal to specify **tunnel mpls traffic-eng backup-bw global-pool Unlimited sub-pool 100**.

To limit the number of both subpool and global pool LSPs, enter the **tunnel mpls traffic-eng backup-bw sub-pool** *kbps* **global-pool** *kbps* command.

The **Unlimited** keyword cannot be used for both the subpool and global pool.

Examples

In the following example, backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. The backup tunnel does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
Router(config)# interface Tunnel1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited
Router(config-if)# end

Router(config)# interface Tunnel2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
Router(config-if)# end
```

Related Commands

Command	Description
mpls traffic-eng backup path	Assigns one or more backup tunnels to a protected interface.

tunnel mpls traffic-eng bandwidth

To configure bandwidth required for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng bandwidth** command in interface configuration mode. To disable this bandwidth configuration, use the **no** form of this command.

tunnel mpls traffic-eng bandwidth [**sub-pool** | **class-type1**] *bandwidth*

no tunnel mpls traffic-eng bandwidth [**sub-pool** | **class-type1**] *bandwidth*

Syntax Description

sub-pool	(Optional) Indicates a subpool tunnel.
class-type1	(Optional) IETF-Standard syntax to indicate a sub-pool tunnel.
bandwidth	The bandwidth, in kilobits per second, set aside for the MPLS traffic engineering tunnel. Range is from 1 to 4294967295.

Defaults

Default bandwidth is 0.
Default is a global pool tunnel.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(11)ST	The **sub-pool** keyword was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was implemented on the Cisco 10000 (PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **class-type1** keyword was added and the **global** keyword was eliminated.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Enter the bandwidth for either a global pool (BC0) or sub-pool (BC1) tunnel, not both in the same statement. To specify both pools, you need to use this command twice, once with the **sub-pool** or **class-type1** keyword to specify the narrower tunnel, and once without those keywords to specify the larger tunnel.

Examples

The following example shows how to configure 100 kbps of bandwidth for the MPLS traffic engineering tunnel:

```
Router(config-if)# tunnel mpls traffic-eng bandwidth 100
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
show mpls traffic-eng tunnel	Displays information about tunnels.

tunnel mpls traffic-eng exp

To specify the experimental (EXP) bits that will be forwarded over a member tunnel that is part of the Class-Based Tunnel Selection (CBTS) bundle, use the **tunnel mpls traffic-eng exp** command in interface configuration mode. To disable forwarding of the EXP bits, use the **no** form of this command.

tunnel mpls traffic-eng exp {*list-of-exp-value*s | **default**}

no tunnel mpls traffic-eng exp {*list-of-exp-values*] | **default**}

Syntax Description

list-of-exp-values	EXP bits allowed for the interface. Enter up to eight EXP values separated by spaces. Values range from 0 to 7. The default is the EXP values that were not configured or a specific member tunnel.
default	The member tunnel will forward the packets with the EXP bits that are not being forwarded by other member tunnels that are part of the same bundle.

Command Default

No EXP value is assigned to a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You should enter the **tunnel mpls traffic-eng exp** command to specify the EXP bits for at least one member tunnel.

With the **tunnel mpls traffic-eng exp** command, you can configure each tunnel with any of the following:

- No EXP-related information
- One or more EXP values for the tunnel to carry (*list-of-exp-values* argument)
- All EXP values not currently allocated to any up tunnel (**default** keyword)
- One or more EXP values for the tunnel to carry, and the property that allows the carrying of all EXP values not currently allocated to any up tunnel (*list-of-exp-values* **default** argument-keyword pair)

The **default** keyword allows you to avoid explicitly listing all possible EXP values. You indicate a preference as to which tunnel to use for certain EXP values, should a tunnel other than the default tunnel go down.

This command allows configurations where:

- Not all EXP values are explicitly allocated to tunnels.
- Multiple tunnels have the default property.
- Some tunnels have EXP values configured and others do not have any configured.
- A given EXP value is configured on multiple tunnels.

The configuration of each tunnel is independent of the configuration of any other tunnel.

Examples

The following example shows how to specify an EXP value of 5 for MPLS TE tunnel Tunnel1:

```
interface Tunnel1
 tunnel destination 10.0.1.1
 tunnel mpls traffic-eng exp 5
```

Related Commands

Command	Description
tunnel mpls traffic-eng exp-bundle master	Configures a master tunnel.
tunnel mpls traffic-eng exp-bundle member	Identifies which tunnel is a member (bundled tunnel) of a master tunnel.

tunnel mpls traffic-eng exp-bundle master

To configure a master tunnel, use the **tunnel mpls traffic-eng exp bundle master** command in interface configuration mode. To unconfigure a master tunnel, use the **no** form of this command.

tunnel mpls traffic-eng exp-bundle master

no tunnel mpls traffic-eng exp-bundle master

Syntax Description

This command has no arguments or keywords.

Command Default

There is no master tunnel for the bundle.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **tunnel mpls traffic-eng exp-bundle master** command to configure a master tunnel. Then specify the **tunnel mpls traffic-eng exp-bundle member** command to identify which tunnels belong to that master tunnel. On the member tunnels, define which experimental (EXP) bit values should be used.

Examples

The following example specifies that there is a master tunnel that includes tunnels Tunnel20000 through Tunnel20007:

```
interface Tunnel200
 ip unnumbered Loopback0
 ip ospf cost 1
 mpls ip
 tunnel destination 10.10.10.10
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel20000
 tunnel mpls traffic-eng exp-bundle member Tunnel20001
 tunnel mpls traffic-eng exp-bundle member Tunnel20002
 tunnel mpls traffic-eng exp-bundle member Tunnel20003
 tunnel mpls traffic-eng exp-bundle member Tunnel20004
 tunnel mpls traffic-eng exp-bundle member Tunnel20005
 tunnel mpls traffic-eng exp-bundle member Tunnel20006
 tunnel mpls traffic-eng exp-bundle member Tunnel20007
```

Related Commands

Command	Description
tunnel mpls traffic-eng exp-bundle member	Identifies which tunnel is a member (bundled tunnel) of a master tunnel.

tunnel mpls traffic-eng exp-bundle member

To identify which tunnel is a member (bundled tunnel) of a master tunnel, use the **tunnel mpls traffic-eng exp-bundle member** command in interface configuration mode. To remove the specified tunnel from being a member of the master tunnel, use the **no** form of this command.

tunnel mpls traffic-eng exp-bundle member *tunnel-number*

no tunnel mpls traffic-eng exp-bundle member *tunnel-number*

Syntax Description

tunnel-number	The tunnel that belongs to a master tunnel.

Command Default

The master tunnel has no member tunnels.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Enter the **tunnel mpls traffic-eng exp-bundle member** command for each tunnel that you want to be a member of the master tunnel. You should enter this command at least once.

Examples

The following example specifies that Tunnel1 is a member of the master tunnel:

```
interface Tunnel200
 ip unnumbered Loopback0
 ip ospf cost 1
 mpls ip
 tunnel destination 10.10.10.10
 tunnel mode mpls traffic-eng
tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel1
```

Related Commands

Command	Description
tunnel mpls traffic-eng exp	Specifies the EXP bits that will be forwarded over a member tunnel that is part of the CBTS bundle.
tunnel mpls traffic-eng exp-bundle master	Configures a master tunnel.

tunnel mpls traffic-eng fast-reroute

To enable a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel to use an established backup tunnel in the event of a link or node failure, use the **tunnel mpls traffic-eng fast-reroute** command in interface configuration mode. To disable this capability, use the **no** form of this command.

tunnel mpls traffic-eng fast-reroute [**bw-protect**] [**node-protection**]

no tunnel mpls traffic-eng fast-reroute

Syntax Description

bw-protect	(Optional) Sets the "bandwidth protection desired" bit so that backup bandwidth protection is enabled.
node-protection	(Optional) Sets the "node protection desired" bit so that backup bandwidth protection is enabled.

Command Default

There is no backup bandwidth protection.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(08)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Cisco Catalyst 6000 series with the SUP720 processor.
12.0(29)S	The **bw-protect** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If you specify the **bw-protect** keyword, all path messages for the tunnel's label-switched path (LSP) are sent with the bandwidth protection bit set.

After you enter the command, with or without the **bw-protect** keyword, the requested action or change propagates along all hops of the LSP. Midpoint routers that are point of local repairs (PLRs) for the LSP take the appropriate action based on whether the bit was just set or cleared. If the bit was just set or cleared, a new backup tunnel selection happens for the LSP because the LSP now has a higher or lower priority in the backup tunnel selection process.

To unconfigure only backup bandwidth protection, enter the **tunnel mpls traffic-eng fast-reroute** command.

To disable an MPLS TE tunnel from using an established backup tunnel in the event of a link or node failure, enter the **no** form of the command.

Examples

In the following example, backup bandwidth protection is enabled:

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
```

Related Commands

Command	Description
mpls traffic-eng backup-path tunnel	Configures the interface to use a backup tunnel in the event of a detected failure on the interface.
mpls traffic-eng fast-reroute backup-prot-preemption	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is not used.
show tunnel mpls traffic-eng fast-reroute	Displays information about fast reroute for MPLS traffic engineering.

tunnel mpls traffic-eng forwarding-adjacency

To advertise a traffic engineering (TE) tunnel as a link in an Interior Gateway Protocol (IGP) network, use the **tunnel mpls traffic-eng forwarding-adjacency** command in interface configuration mode. To disable the functionality, use the **no** form of this command.

tunnel mpls traffic-eng forwarding-adjacency [**holdtime** *milliseconds*]

no tunnel mpls traffic-eng forwarding-adjacency

Syntax Description

holdtime *milliseconds*	(Optional) Specifies the time, in milliseconds (ms), that a TE tunnel waits after going down before informing the network. The range is 0 to 4294967295 ms. The default value is 0.

Command Default

A TE tunnel is not advertised as a link in an IGP network.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.0(16)ST	This command was integrated into Cisco IOS Release 12.0(16)ST.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **tunnel mpls traffic-eng forwarding-adjacency** command with the **isis metric** command to avoid inefficient forwarding behavior. Ensure that any nodes traversed by the TE tunnel being advertised do not consider the TE tunnel as part of the shortest path to the destination.

Note The **tunnel mpls traffic-eng forwarding-adjacency** command requires Intermediate System-to-Intermediate System (IS-IS) support.

Examples

In the following example, the holdtime is set to 10,000 milliseconds:

```
Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency holdtime 10000
```

In the following example, the holdtime defaults to 0:

```
Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency
```

Related Commands

Command	Description
debug mpls traffic-eng forwarding-adjacency	Displays debug messages for traffic engineering, forwarding adjacency events.
isis metric	Configures the cost metric for an interface.
show mpls traffic-eng forwarding-adjacency	Displays TE tunnels being advertised as links in an IGP network.

tunnel mpls traffic-eng interface down delay

To force a tunnel to go down as soon as the headend router detects that the label-switched path (LSP) is down, use the **tunnel mpls traffic-eng interface down delay** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng interface down delay *time*

no tunnel mpls traffic-eng interface down delay *time*

Syntax Description

time	Time, in minutes. The only valid value is 0.

Defaults

There is a delay before the tunnel goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You cannot specify both the **tunnel mpls traffic-eng interface down delay** command and the **tunnel mpls traffic-eng forwarding-adjacency** command. The first command that you enter would prevent the implementation of the other command and would cause the system to display error messages.

Examples

In the following example, if the headend router detects that a link has goes down on tunnel 1000, the tunnel goes down immediately.

```
Router(config)# interface tunnel 1000
Router(config-if)# tunnel mpls traffic-eng interface down delay 0
```

tunnel mpls traffic-eng load-share

To determine load-sharing among two or more Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels that begin at the same router and go to an identical destination, use the **tunnel mpls traffic-eng load-share** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng load-share *value*

no tunnel mpls traffic-eng load-share *value*

Syntax Description

value	A value from which the head-end router will calculate the proportion of traffic to be sent down each of the parallel tunnels. Range is from 1 to 1000000.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each parallel tunnel must be configured with this command. Specify a value to indicate the *proportion* of total traffic you want to be allocated into each individual tunnel. For example, if there are to be three parallel tunnels, and you want Tunnel1 to carry half of the traffic and the other two tunnels to carry one-quarter, you should enter the following values:

- Tunnel1 — 2
- Tunnel2 — 1
- Tunnel3 — 1

The ability to divide bandwidth in unequal amounts across traffic engineering tunnels has a finite granularity. This granularity varies by platform, with both hardware and software limits. If load-sharing is configured so that it exceeds the available granularity, the following message is displayed:

```
@FIB-4-UNEQUAL: Range of unequal path weightings too large for prefix x.x.x.x/y. Some
available paths may not be used.
```

To eliminate this message, it is recommended that you change the requested bandwidth or loadshare.

Examples

In the following example, three tunnels are configured, with the first tunnel receiving half of the traffic and the other two tunnels receiving one-quarter:

```
interface Tunnel1
    ip unnumbered Loopback0
    no ip directed-broadcast
    tunnel destination 41.41.41.41
    tunnel mode mpls traffic-eng
    tunnel mpls traffic-eng path-option 10 dynamic
    tunnel mpls traffic-eng load-share 2

interface Tunnel2
    ip unnumbered Loopback0
    no ip directed-broadcast
    tunnel destination 41.41.41.41
    tunnel mode mpls traffic-eng
    tunnel mpls traffic-eng path-option 10 dynamic
    tunnel mpls traffic-eng load-share 1

interface Tunnel3
    ip unnumbered Loopback0
    no ip directed-broadcast
    tunnel destination 41.41.41.41
    tunnel mode mpls traffic-eng
    tunnel mpls traffic-eng path-option 10 dynamic
    tunnel mpls traffic-eng load-share 1
```

Related Commands

Command	Description
show ip route	Displays routing table information about tunnels, including their traffic share.
tunnel mpls traffic-eng bandwidth	Configures bandwidth in Kbps for an MPLS traffic engineering tunnel.

tunnel mpls traffic-eng path-option

To configure a path option for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng path-option** command in interface configuration mode. To disable this function, use the **no** form of this command.

tunnel mpls traffic-eng path-option *number* { **dynamic** | **explicit** {{**name** *path-name* | **identifier** *path-number*} **[verbatim]**}} [**attributes** *name*] [**bandwidth {***bandwidth* **| sub-pool }**] [**lockdown**]

no tunnel mpls traffic-eng path-option { *number* | **protect** *number* }

Syntax Description

number	Preference for this path option. When you configure multiple path options, lower numbered options are preferred. Valid values are from 1 to 1000.
dynamic	Path of the label switched path (LSP) is dynamically calculated.
explicit	Path of the LSP is an IP explicit path.
name *path-name*	Path name of the IP explicit path that the tunnel uses with this option.
identifier *path-number*	Path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535.
lockdown	(Optional) The LSP cannot be reoptimized.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can configure multiple path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. Path setup preference is for lower (not higher) numbers, so option 1 is preferred.

If you specify the **dynamic** keyword, the software checks both the physical bandwidth of the interface and the available TE bandwidth to be sure that the requested amount of bandwidth does not exceed the physical bandwidth of any link. To oversubscribe links, you must specify the **explicit** keyword. If you use the **explicit** keyword, the software only checks how much bandwidth is available on the link for TE; the amount of bandwidth you configure is not limited to how much physical bandwidth is available on the link.

Examples

The following example shows how to configure the tunnel to use a named IP explicit path:

```
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test
```

Related Commands

Command	Description
ip explicit-path	Enters the command mode for IP explicit paths and creates or modifies the specified path.
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng path-option protect	Configures a secondary path option for an MPLS TE tunnel.

tunnel mpls traffic-eng path-option protect

To configure a secondary path option for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng path-option protect** command in interface configuration mode. To disable this function, use the **no** form of this command.

tunnel mpls traffic-eng path-option protect *number* {**dynamic** [**attributes** *lsp-attributes* | **bandwidth** {*kbps* | **subpool** *kbps*} [**lockdown**] | **lockdown** [**bandwidth** {*kbps* | **subpool** *kbps*} | **explicit** {**identifier** *path-number* | **name** *path-name*} [**attributes** *lsp-attributes* [**verbatim**] | **bandwidth** {*kbps* | **subpool** *kbps*} [**lockdown**] [**verbatim**] | **lockdown bandwidth** {*kbps* | **subpool** *kbps*} [**lockdown**] [**verbatim**] | **verbatim** [**lockdown**]]}

no tunnel mpls traffic-eng path-option protect *number*

Syntax Description

number	The primary path option being protected. Valid values are from 1 to 1000.
dynamic	Part of the label switched path (LSP) is dynamically calculated.
attributes *lsp-attributes*	(Optional) Identifies an LSP attribute list. **Note** The attribute list used should be the same as the primary path option being protected.
bandwidth *kbps*	(Optional) Overrides the bandwidth configured on the tunnel or the attribute list. The value *kbps* is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. **Note** The bandwidth value should be the same as the primary path option being protected.
subpool *kbps*	(Optional) Indicates that the bandwidth override value uses subpool bandwidth. The value *kbps* is the number of kilobits per second of subpool bandwidth set aside for the path option. The range is from 1 to 4294967295.
lockdown	(Optional) The LSP cannot be reoptimized.
explicit	Path of the LSP is an IP explicit path.
identifier *path-number*	Path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535.
name *path-name*	Path name of the IP explicit path that the tunnel uses with this option.
verbatim	(Optional) Bypasses the topology database verification process.

Command Default

The MPLS TE tunnel does not have a secondary path option.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(26)S	LSP-related keywords and arguments for path options were added.
12.0(30)S	The **protect** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Cisco recommends that the primary path options being protected use explicit paths.

Calculation of a dynamic path for the path protected LSP is not available. When configuring the IP explicit path for the path protected LSP, choose hops that minimize the number of links and nodes shared with the primary path option that is being protected.

If the path option being protected uses an attribute list, configure path protection to use the same attribute list.

If the path option being protected uses bandwidth override, configure path protection to use bandwidth override with the same values.

Examples

The following example shows how to configure the tunnel to use a named IP explicit path:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 1 explicit name test
```

The following example shows how to configure path option 1 to use an LSP attribute list identified with the numeral 1:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 1 explicit name test
attributes 1
```

The following example shows how to configure bandwidth for a path option to override the bandwidth configured on the tunnel:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 3 explicit name test
bandwidth 0
```

Related Commands

Command	Description
ip explicit-path	Enters the command mode for IP explicit paths and creates or modifies the specified path.
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng path-option	Configures a primary path for an MPLS TE tunnel.

tunnel mpls traffic-eng path-selection metric

To specify the metric type to use for path calculation for a tunnel, use the **tunnel mpls traffic-eng path-selection metric** command in interface configuration mode. To remove the specified metric type, use the **no** form of this command.

tunnel mpls traffic-eng path-selection metric {**igp** | **te**}

no tunnel mpls traffic-eng path-selection metric

Syntax Description

igp	Use the Interior Gateway Protocol (IGP) metric.
te	Use the traffic engineering (TE) metric.

Defaults

The default is the **te** metric.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the **tunnel mpls traffic-eng path-selection metric** command was entered to specify a metric type for the tunnel, use that metric type.
- Otherwise, if the **mpls traffic-eng path-selection metric** was entered to specify a metric type, use that metric type.
- Otherwise, use the default (**te**) metric.

Examples

The following commands specify that the igp metric should be used when you are calculating the path for Tunnel102:

```
Router(config)# interface tunnel102
Router(config-if)# tunnel mpls traffic-eng path-selection metric igp
```

Related Commands

Command	Description
mpls traffic-eng path-selection metric	Specifies the metric type to use for path calculation for TE tunnels for which no metric has been explicitly configured.

tunnel mpls traffic-eng priority

To configure the setup and reservation priority for an Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng priority** command in interface configuration mode. To remove the specified setup and reservation priority, use the **no** form of this command.

tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]

no tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]

Syntax Description

setup-priority	The priority used when signalling an LSP for this tunnel to determine which existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
hold-priority	(Optional) The priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signalled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

Defaults

setup-priority: 7
hold-priority: The same value as the setup-priority

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a label switched path (LSP) is being signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software preempts lower-priority LSPs so that the new LSP can be admitted. (LSPs are preempted if that allows the new LSP to be admitted.)

In the described determination, the new LSP's priority is its setup priority and the existing LSP's priority is its hold priority. The two priorities make it possible to signal an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) but a high hold priority (so that the LSP is not preempted after it is established).

Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

Examples

The following example shows how to configure a tunnel with a setup and hold priority of 1:

```
Router(config-if)# tunnel mpls traffic-eng priority 1
```

Related Commands

Command	Description
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng record-route

To include the interface address for the label switched path (LSP) in the Record Route Object (RRO) for an RESV message, use the **tunnel mpls traffic-eng record-route** command in interface configuration mode. To remove the interface address for the LSP in the RRO for the RESV message, use the **no** form of this command.

tunnel mpls traffic-eng record-route

no tunnel mpls traffic-eng record-route

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is disabled. The interface addresses for the LSP are not included in the RRO of the RESVmessage.The **record-route** option is automatically enabled when the **tunnel mpls traffic-eng fast-reroute** command for the fast-reroute (FRR) feature is enabled at the headend.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

The RRO has two functions. It records the route of the LSP that can be used in loop prevention, and it records labels that are used by FRR.

The contents of a RRO are a series of variable-length data items called subobjects.

If record route is enabled, the RRO contains details in the following order: node-ID, interface address, and label.

Examples

The following example shows how to include the interface address using the **tunnel mpls traffic-eng record-route** command:

```
interface tunnel1
ip unnumbered loopback0
no ip direct-broadcast
tunnel destination 192.168.1.5
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng record-route
```

Related Commands,

Command	Description
show ip rsvp reservation	Displays current RSVP related receiver information in the database.
show mpls traffic-eng tunnels	Displays information on the source, destination, path and interface of MPLS TE tunnels.
tunnel mpls traffic-eng fast-reroute	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

tunnel tsp-hop

To define hops in the path for the label switching tunnel, use the **tunnel tsp-hop** command in interface configuration mode. To remove these hops, use the **no** form of this command.

tunnel tsp-hop *hop-number ip-address* [**lasthop**]

no tunnel tsp-hop *hop-number ip-address* [**lasthop**]

Syntax Description

hop-number	The sequence number of the hop being defined in the path. The first number is 1, which identifies the hop just after the head hop.
ip-address	The IP address of the input interface on that hop.
lasthop	(Optional) Indicates that the hop being defined is the final hop in the path (the tunnel destination).

Defaults

No hops are defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The list of tunnel hops must specify a strict source route for the tunnel. In other words, the router at hop <*n*> must be directly connected to the router at hop <*n*>+1.

Examples

The following example shows how to configure a two-hop tunnel. The first hop router/switch is 172.16.0.2, and the second and last hop is router/switch 172.17.0.2.

```
Router(config)# interface tunnel 5

Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# ip unnumbered e0/1
Router(config-if)# tunnel tsp-hop 1 172.16.0.2
Router(config-if)# tunnel tsp-hop 2 172.17.0.2 lasthop
```

Related Commands

Command	Description
tunnel mpls traffic-eng affinity	Sets the encapsulation mode of the tunnel to label switching.

vpn id

To set or update a Virtual Private Network (VPN) ID on a VPN routing and forwarding (VRF) instance, use the **vpn id** command in VRF configuration mode.

vpn id *oui*:*vpn-index*

Syntax Description

oui:	Organizationally unique identifier (OUI). The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets and followed by a colon.
vpn-index	Identifies the VPN within the company. This VPN index is restricted to four octets.

Defaults

The VPN ID is not set.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(17)ST	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each VRF configured in a provider edge (PE) router can have a VPN ID. Use the same VPN ID for the PE routers that belong to the same VPN. Make sure the VPN ID is unique for each VPN in the service provider network.

Once configured, a VPN ID cannot be removed, however, it can be changed. To change the VPN ID, issue the command again. The new ID overwrites the existing ID.

Examples

The following example shows how to assign the VPN ID of 0000a100003f6c to a VRF called vpn1:

```
Router(config)# ip vrf vpn1
Router(config-vrf)# vpn id a1:3f6c
```

Related Commands

Command	Description
show ip vrf detail	Displays all the VRFs on a router.
show ip vrf id	Displays all the VPN IDs that are configured in the router and their associated VRF names and VRF RDs.

vrf definition

To configure a Virtual Private Network (VPN) routing and forwarding (VRF) routing table instance and enter VRF configuration mode, use the **vrf definition** command in global configuration mode. To remove a VRF routing table, use the **no** form of this command.

vrf definition *vrf-name*

no vrf definition *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined.
No import or export lists are associated with a VRF.
No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **vrf definition** command to give a VRF a name and to enter VRF configuration mode. Once the router is in VRF configuration mode, use the **rd** command to give the VRF a route distinguisher (RD). The **rd** command creates the routing and forwarding tables and associates the RD with the VRF instance named in the *vrf-name* argument.

Users can configure shared route targets (import and export) between IPv4 and IPv6. This feature is useful in a migration scenario, where IPv4 policies already are configured and IPv6 policies should be the same as the IPv4 policies. You can configure separate route-target policies for IPv4 and IPv6 VPNs in address family configuration mode. Enter address family configuration mode from VRF configuration mode.

In VRF configuration mode, you can also associate a Simple Network Management Protocol (SNMP) context with the named VRF and configure or update a VPN ID.

The **vrf definition default** command can be used to configure a VRF name that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example assigns the name vrf1 to a VRF, enters VRF configuration mode, and configures a route distinguisher, 100:20:

```
Router(config)# vrf definition vrf1
Router(config-vrf)# rd 100:20
```

Related Commands

Command	Description
address-family	Enters address family configuration mode for configuring routing protocols such as BGP, RIP, and static routing.
context	Associates an SNMP context with a particular VRF.
rd	Specifies a route distinguisher.
route-target	Creates a route-target extended community for a VPN VRF.
vpn id	Sets or updates a VPN ID on a VRF.
vrf forwarding	Associates a VRF instance with an interface or subinterface.

vrf forwarding

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with an interface or subinterface, use the **vrf forwarding** command in interface configuration mode. To disassociate a VRF from an interface, use the **no** form of this command.

vrf forwarding *vrf-name*

no vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default for an interface is the global routing table.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **vrf forwarding** command to associate an interface with a VRF. When the interface is bound to a VRF, previously configured IPv4 and IPv6 addresses are removed, and they must be reconfigured.

Examples

The following example shows how to associate a VRF named site1 to serial interface 0/0 and configure an IPv6 and an IPv4 address:

```
interface Serial0/0
 vrf forwarding site1
 ipv6 address 2001:100:1:1000::72b/64
 ip address 10.11.11.1 255.255.255.0
```

Related Commands

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

vrf selection source

To populate a single source IP address, or range of source IP addresses, to a VRF Selection table, use the **vrf selection source** command in global configuration mode. To remove a single source IP address or range of source IP addresses from a VRF Selection table, use the **no** form of this command.

vrf selection source *source-IP-address source-IP-mask* **vrf** *vrf-name*

no vrf selection source *source-IP-address source-IP-mask* **vrf** *vrf-name*

Syntax Description

source-IP-address	New source IP address to be added to the VRF Selection table.
source-IP-mask	IP mask for the source IP address or range of single source IP addresses to be added to the VRF Selection table.
vrf *vrf-name*	Name of the VRF Selection table to which the single source IP address or range of source IP addresses should be added.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a VRF table is removed by using the **no ip vrf** *vrf-name* command in global configuration mode, all configurations associated with that VRF will be removed including those configurations added with the **vrf selection source** command.

Examples

The following example shows how to populate the VRF Selection table vpn1 with a source IP network address 10.0.0.0 and the IP mask 255.0.0.0, which would forward any packets with the source IP address 10.0.0.0 into the VRF instance vpn1:

```
Router(config)# vrf selection source 10.0.0.0 255.0.0.0 vrf vpn1
```

The following example shows the message you receive after you have removed the source IP network address 107.1.1.1 and the IP mask 255.255.255.255 from the VRF Selection table vpn1:

```
Router (config)# no vrf selection source 10.1.1.1 255.255.255.255 vrf vpn1
Router (config)#
VRF Selection Configuration: addr:10.1.1.1, mask:255.255.255.255, vrf_name:vpn1

5d13h: VRF Selection Remove Configuration: addr:10.1.1.1, mask: 255.255.255.255
Router (config)#
```

The following example shows the message you receive after you have added the source IP network address 10.1.1.1 and the IP mask 255.255.255.255 to the VRF Selection table vpn1:

```
Router (config)# vrf selection source 10.1.1.1 255.255.255.255 vrf vpn1
Router (config)#
VRF Selection Configuration: addr:10.1.1.1, mask:255.255.255.255, vrf_name:vpn1
VRF Selection: VRF table vpn1, id is: 1
```

Related Commands

Command	Description
ip vrf receive	Adds all the IP addresses that are associated with an interface into a VRF table.
ip vrf select source	Enables VRF Selection on an interface.

vrf upgrade-cli

To upgrade a Virtual Private Network (VPN) routing and forwarding (VRF) instance or all VRFs on the router to support multiple address families (multi-AFs) for the same VRF, use the **vrf upgrade-cli** command in global configuration mode.

vrf upgrade-cli multi-af-mode {**common-policies** | **non-common-policies**} [**vrf** *vrf-name*]

Syntax Description

multi-af-mode	Specifies an upgrade of a single-protocol VRF or all VRFs to a multiprotocol VRF that supports multi-AFs configuration.
common-policies	Specifies to copy the route-target policies to the common part of the VRF configuration so that the policies apply to all address families configured in the multi-AF VRF.
non-common-policies	Specifies to copy the route-target policies to the IPv4 address family part of the VRF configuration so that the policies apply only to an IPv4 VRF.
vrf	(Optional) Specifies a VRF for the upgrade to a multi-AF VRF configuration.
vrf-name	(Optional) The name of the single-protocol VRF to upgrade to a multi-AF VRF configuration.

Command Default

If you do not enter the name of a specific single-protocol VRF, all VRFs defined on the router are upgraded to the multi-AF VRF configuration.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **vrf upgrade-cli** command is used to upgrade a specified single-protocol VRF (IPv4-only VRF) configuration or all single-protocol VRF configurations on the router to a multiprotocol VRF that supports multi-AF configuration.

The upgrade is automatic and does not require any further configuration. After you enter the **vrf upgrade-cli** command, the single-protocol VRF configuration is lost when you save the configuration to NVRAM. A multiprotocol VRF configuration is saved.

If your configuration requires that all route-target policies (import, export, both) apply to all address families, you enter the **vrf upgrade-cli multi-af-mode common-policies** command. If your configuration requires that these policies apply to IPv4 VPNs only, enter the **vrf upgrade-cli multi-af-mode non-common-policies** command.

After the upgrade to a multiprotocol VRF is complete, you can edit the VRF only with multiprotocol VRF configuration commands.

Examples

The following example shows how to upgrade a single-protocol VRF configuration named vrf1 to a multi-AF VRF configuration and apply the common policies of vrf1 to all address families defined for the VRF:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
Router(config)# vrf upgrade-cli multi-af-mode common-policies vrf vrf1

You are about to upgrade to the multi-AF VRF syntax commands.
You will loose any IPv6 address configured on interfaces
belonging to upgraded VRFs.
Are you sure ? [yes]: yes
Number of VRFs upgraded: 1
Router(config)# exit
```

The following is an example of the single-protocol VRF configuration for VRF vrf1 before you enter the **vrf upgrade-cli** command to upgrade to a multi-AF multiprotocol VRF configuration:

```
!
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1

interface Loopback1
 ip vrf forwarding vrf1
 ip address 10.3.3.3 255.255.255.255
```

This is an example of the multi-AF multiprotocol VRF configuration for VRF vrf1 after you enter the **vrf upgrade-cli** command with the **common-policies** keyword:

```
!
vrf definition vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
 exit-address-family
!

interface Loopback1
 vrf forwarding vrf1
 ip address 10.3.3.3 255.255.255.255
```

Related Commands

Command	Description
show vrf	Displays the defined VRF instances.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.
vrf forwarding	Associates a VRF instance with an interface or subinterface.

xconnect

To bind an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire, use the **xconnect** command in one of the supported configuration modes. To restore the default values, use the **no** form of this command.

xconnect *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | **pw-class** *pw-class-name* }[**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]

no xconnect

Cisco uBR10012 Router and Cisco uBR7200 Series Universal Broadband Routers

xconnect *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*]

no xconnect *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*]

Syntax Description

peer-ip-address	IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.
vc-id	The 32-bit identifier of the virtual circuit (VC) between the PE routers.
encapsulation {**l2tpv3** [**manual**] | **mpls** [**manual**]}	Specifies the tunneling method to encapsulate the data in the pseudowire: • **l2tpv3**—Specifies Layer 2 Tunneling Protocol, version 3 (L2TPv3) as the tunneling method. • **mpls**—Specifies Multiprotocol Label Switching (MPLS) as the tunneling method. • **manual**—Specifies that no signaling is to be used in the attachment circuit. This keyword places the router in xconnect configuration mode for manual configuration of the attachment circuit. Use this keyword to manually configure an AToM or L2TPv3 static pseudowire.
pw-class *pw-class-name*	(Optional) Specifies the pseudowire class for advanced configuration.
sequencing	(Optional) Sets the sequencing method to be used for packets received or sent. This keyword is not supported with the AToM Static Pseudowire Provisioning feature.
transmit	Sequences data packets received from the attachment circuit.
receive	Sequences data packets sent into the attachment circuit.
both	Sequences data packets that are both sent and received from the attachment circuit.
pw-type	(Optional) Pseudowire type. You can specify one of the following types: • 4—Specifies Ethernet VLAN. • 5—Specifies Ethernet port.

Command Default

The attachment circuit is not bound to the pseudowire.

Command Modes

Connect configuration
Interface configuration (config-if)
l2transport configuration (for ATM)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.0(28)S	Support was added for Multilink Frame Relay connections.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was updated to add support for AToM static pseudowires, and so that the remote router ID need not be the Label Distribution Protocol (LDP) router ID of the peer.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each xconnect configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

Note If the remote router is a Cisco 12000 series Internet router, the *peer-ip-address* argument must specify a loopback address on that router.

The same *vcid* value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE router. The VC ID creates the binding between a pseudowire and an attachment circuit.

With the introduction of VPLS Autodiscovery in Cisco IOS Release 12.2(33)SRB, the remote router ID need not be the LDP router ID. The address you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Note The VPLS Autodiscovery feature is not supported with L2TPv3.

For L2TPv3, to manually configure the settings used in the attachment circuit, use the **manual** keyword in the **xconnect** command. This configuration is called a static session. The router is placed in xconnect configuration mode, and you can then configure the following options:

- Local and remote session identifiers (using the **l2tp id** command) for local and remote PE routers at each end of the session.
- Size of the cookie field used in the L2TPv3 headers of incoming (sent) packets from the remote PE peer router (using the **l2tp cookie local** command).
- Size of the cookie field used in the L2TPv3 headers of outgoing (received) L2TP data packets (using the **l2tp cookie remote** command).
- Interval used between sending hello keepalive messages (using the **l2tp hello** command).

For L2TPv3, if you do not enter the **encapsulation l2tpv3 manual** keywords in the **xconnect** command, the data encapsulation type for the L2TPv3 session is taken from the encapsulation type configured for the pseudowire class specified with the **pseudowire-class** *pw-class-name* command.

The **pw-class** keyword with the *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **xconnect** command.

Software prior to Cisco IOS Release 12.2(33)SRB configured pseudowires dynamically using Label Distribution Protocol (LDP) or another directed control protocol to exchange the various parameters required for these connections. In environments that do not or cannot use directed control protocols, the **xconnect** command allows provisioning an AToM static pseudowire. Use the **manual** keyword in the **xconnect** command to place the router in xconnect configuration mode. MPLS pseudowire labels are configured using the **mpls label** and (optionally) **mpls control-word** commands in xconnect configuration mode.

Examples

The following example configures xconnect service for an Ethernet interface by binding the Ethernet circuit to the pseudowire named 123 with a remote peer 10.0.3.201. The configuration settings in the pseudowire class named vlan-xconnect are used.

```
Router(config)# interface Ethernet0/0.1
Router(config-if)# xconnect 10.0.3.201 123 pw-class vlan-xconnect
```

The following example enters xconnect configuration mode and manually configures L2TPv3 parameters for the attachment circuit:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn) l2tp id 222 111
Router(config-if-xconn) l2tp cookie local 4 54321
Router(config-if-xconn) l2tp cookie remote 4 12345
Router(config-if-xconn) l2tp hello l2tp-defaults
```

The following example enters xconnect configuration mode and manually configures an AToM static pseudowire. The example shows the configuration for only one side of the connection; the configurations on each side of the connection must be symmetrical.

```
Router# configure terminal
Router(config)# interface Ethernet1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.131.191.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# exit
Router(config-if)# exit
```

The following example shows how to bind an attachment circuit to a pseudowire and configure an AToM service on a Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# cable l2vpn 0000.396e.6a68 customer1
Router(config-l2vpn)# service instance 2000 Ethernet
Router(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming packets received from the remote PE peer router.
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing packets sent from the local PE peer router.
l2tp hello	Specifies the use of a hello keepalive setting contained in a specified L2TP class configuration for a static L2TPv3 session.
l2tp id	Configures the identifiers used by the local and remote provider edge routers at each end of an L2TPv3 session.
l2tp-class	Configures a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes.
mpls control-word	Enables the MPLS control word in an AToM static pseudowire connection.
mpls label	Configures an AToM static pseudowire connection by defining local and remote pseudowire labels.
mpls label range	Configures the range of local labels available for use on packet interfaces.
pseudowire-class	Configures a template of pseudowire configuration settings used by the attachment circuits transported over a pseudowire.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

xconnect logging pseudowire status

To enable system logging (syslog) reporting of pseudowire status events, use the **xconnect logging pseudowire status** command in global configuration mode. To disable syslog reporting of pseudowire status events, use the **no** form of this command.

xconnect logging pseudowire status

no xconnect logging pseudowire status

Syntax Description

This command has no arguments or keywords.

Defaults

Syslog reporting of pseudowire status events is off.

Command Modes

Global configuration

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

Use this command to enable syslog reporting of pseudowire status events.

Examples

The following example enables syslog reporting of pseudowire status events:

```
xconnect logging pseudowire status
```

Related Commands

Command	Description
xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to a L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.