Cisco IOS Switching Services Command Reference

Release 12.2

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

Customer Order Number: DOC-7811750=
Text Part Number: 78-11750-02

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.

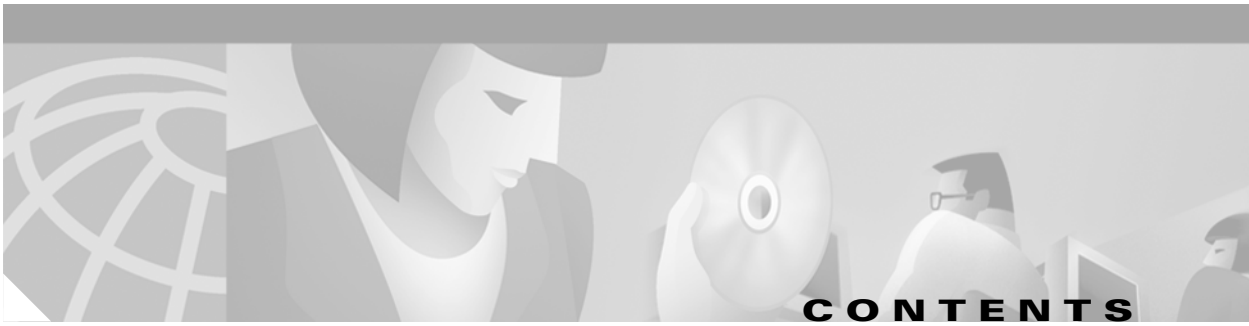
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Discover All That's Possible, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site 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. (0101R)

Cisco IOS Switching Services Command Reference
© 2002– 2006 Cisco Systems, Inc.
All rights reserved.



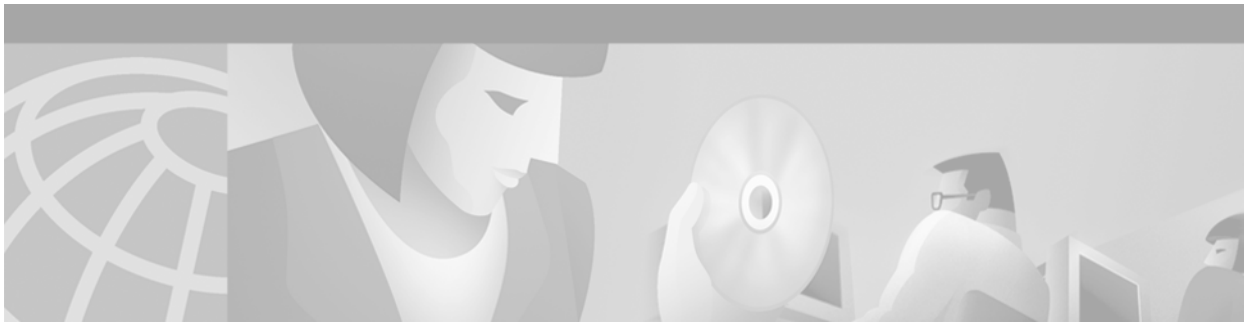
CONTENTS

About Cisco IOS Software Documentation v

Using Cisco IOS Software xiii

Cisco IOS Switching Commands XR-1

INDEX



About Cisco IOS Software Documentation

This chapter discusses the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation from Cisco Systems.

Documentation Objectives

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

Audience

The Cisco IOS software documentation set is intended primarily for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the tasks, the relationship between tasks, or the Cisco IOS software commands necessary to perform particular tasks. The Cisco IOS software 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 software release.

Documentation Organization

The Cisco IOS software documentation set consists of documentation modules and master indexes. In addition to the main documentation set, there are supporting documents and resources.

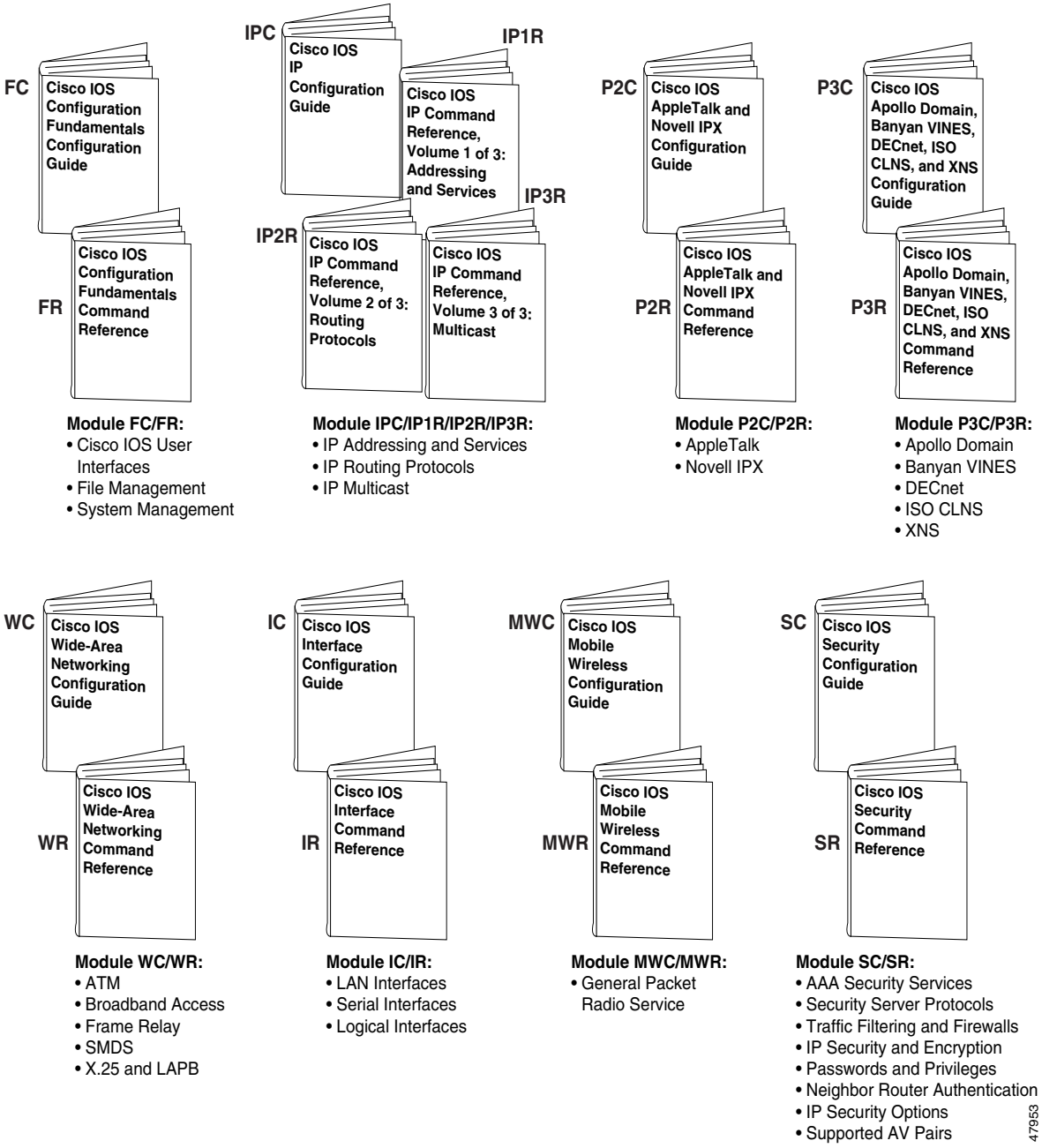
Documentation Modules

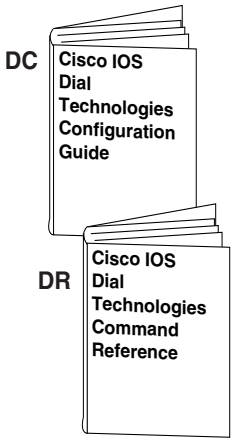
The Cisco IOS documentation modules consist of configuration guides and corresponding command reference publications. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference publication provide complete Cisco IOS command syntax information. Use each configuration guide in conjunction with its corresponding command reference publication.

Figure 1 shows the Cisco IOS software documentation modules.

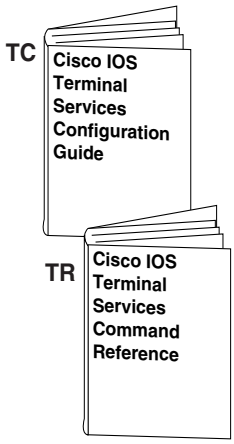
Note The abbreviations (for example, FC and FR) next to the book icons are page designators, which are defined in a key in the index of each document to help you with navigation. The bullets under each module list the major technology areas discussed in the corresponding books.

Figure 1 Cisco IOS Software Documentation Modules

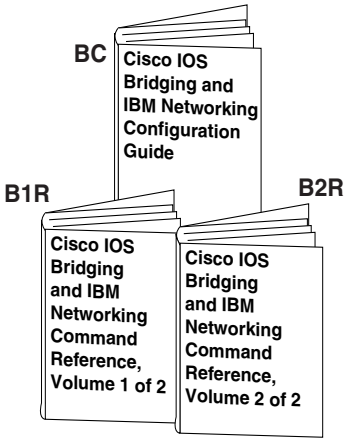




Module DC/DR:
- Preparing for Dial Access
- Modem and Dial Shelf Configuration and Management
- ISDN Configuration
- Signalling Configuration
- Dial-on-Demand Routing Configuration
- Dial-Backup Configuration
- Dial-Related Addressing Services
- Virtual Templates, Profiles, and Networks
- PPP Configuration
- Callback and Bandwidth Allocation Configuration
- Dial Access Specialized Features
- Dial Access Scenarios

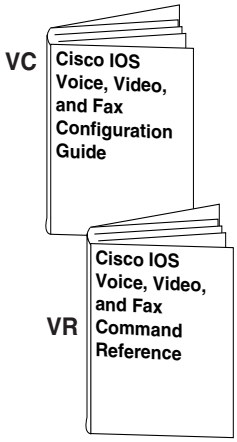


Module TC/TR:
- ARA
- LAT
- NASI
- Telnet
- TN3270
- XRemote
- X.28 PAD
- Protocol Translation

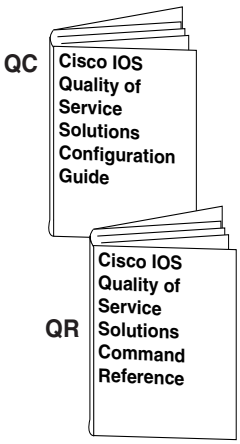


Module BC/B1R:
- Transparent Bridging
- SRB
- Token Ring Inter-Switch Link
- Token Ring Route Switch Module
- RSRB
- DLSw+
- Serial Tunnel and Block Serial Tunnel
- LLC2 and SDLC
- IBM Network Media Translation
- SNA Frame Relay Access
- NCIA Client/Server
- Airline Product Set

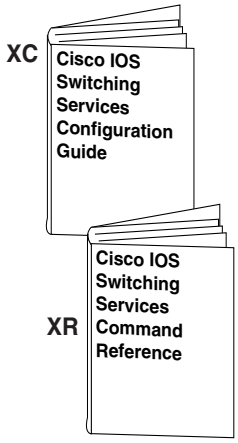
Module BC/B2R:
- DSPU and SNA Service Point
- SNA Switching Services
- Cisco Transaction Connection
- Cisco Mainframe Channel Connection
- CLAW and TCP/IP Offload
- CSNA, CMPC, and CMPC+
- TN3270 Server



Module VC/VR:
- Voice over IP
- Call Control Signalling
- Voice over Frame Relay
- Voice over ATM
- Telephony Applications
- Trunk Management
- Fax, Video, and Modem Support



Module QC/QR:
- Packet Classification
- Congestion Management
- Congestion Avoidance
- Policing and Shaping
- Signalling
- Link Efficiency Mechanisms



Module XC/XR:
- Cisco IOS Switching Paths
- NetFlow Switching
- Multiprotocol Label Switching
- Multilayer Switching
- Multicast Distributed Switching
- Virtual LANs
- LAN Emulation

47954

Master Indexes

Two master indexes provide indexing information for the Cisco IOS software documentation set: an index for the configuration guides and an index for the command references. Individual books also contain a book-specific index.

The master indexes provide a quick way for you to find a command when you know the command name but not which module contains the command. When you use the online master indexes, you can click the page number for an index entry and go to that page in the online document.

Supporting Documents and Resources

The following documents and resources support the Cisco IOS software documentation set:

- *Cisco IOS Command Summary* (two volumes)—This publication explains the function and syntax of the Cisco IOS software commands. For more information about defaults and usage guidelines, refer to the Cisco IOS command reference publications.
- *Cisco IOS System Error Messages*—This publication lists and describes Cisco IOS system error messages. Not all system error messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
- *Cisco IOS Debug Command Reference*—This publication contains an alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, usage guidelines, and sample output.
- *Dictionary of Internetworking Terms and Acronyms*—This Cisco publication compiles and defines the terms and acronyms used in the internetworking industry.
- New feature documentation—The Cisco IOS software documentation set documents the mainline release of Cisco IOS software (for example, Cisco IOS Release 12.2). New software features are introduced in early deployment releases (for example, the Cisco IOS "T" release train for 12.2, 12.2(x)T). Documentation for these new features can be found in standalone documents called "feature modules." Feature module documentation describes new Cisco IOS software and hardware networking functionality and is available on Cisco.com and the Documentation CD-ROM.
- Release notes—This documentation describes system requirements, provides information about new and changed features, and includes other useful information about specific software releases. See the section "Using Software Release Notes" in the chapter "Using Cisco IOS Software" for more information.
- Caveats documentation—This documentation provides information about Cisco IOS software defects in specific software releases.
- RFCs—RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained on the World Wide Web at http://www.rfc-editor.org/.
- MIBs—MIBs are used for network monitoring. For lists of supported MIBs by platform and release, and to download MIB files, see the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

New and Changed Information

Since the last release of the *Cisco IOS Switching Services Command Reference*, the term ‘quality of service’ (QoS) replaces the term ‘class of service’ (CoS). All references to Multiprotocol Label Switching (MPLS) CoS functionality has been replaced by the MPLS QoS functionality., which is documented in the “Multiprotocol Label Switching Overview” chapter and the “Configuring Multiprotocol Label Switching” chapter.

Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means 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 an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`boldface screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

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 materials not contained in this manual.

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

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at the following website:

http://www.cisco.com

Translated documentation is available at the following website:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation can be ordered in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

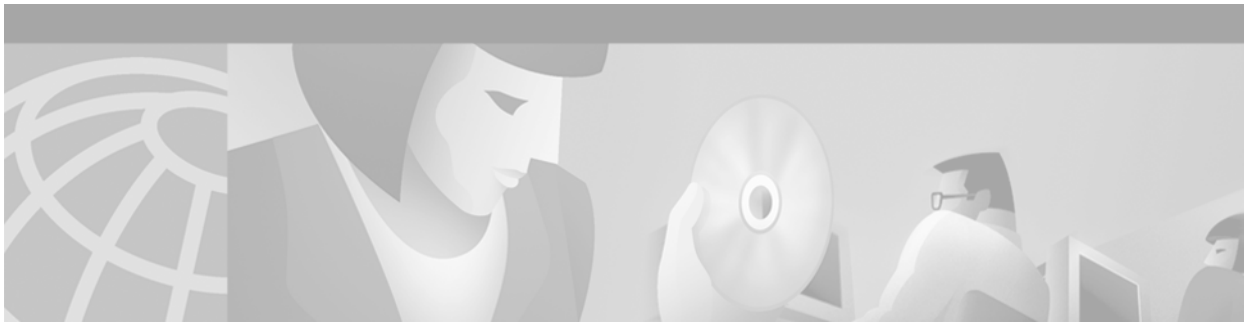
Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



Using Cisco IOS Software

This chapter provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

- Understanding Command Modes
- Getting Help
- Using the no and default Forms of Commands
- Saving Configuration Changes
- Filtering Output from the show and more Commands
- Identifying Supported Platforms

For an overview of Cisco IOS software configuration, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information on the conventions used in the Cisco IOS software documentation set, see the chapter "About Cisco IOS Software Documentation" located at the beginning of this book.

Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS 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.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command, or press **Ctrl-Z**.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command, or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (**?**) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

Table 2 How to Find Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to `Router#`.

`Router# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router(config)#`.

`Router(config)# interface serial ?`
`  <0-6>  Serial interface number`
`Router(config)# interface serial 4 ?`
`  /`
`Router(config)# interface serial 4/ ?`
`  <0-3>  Serial interface number`
`Router(config)# interface serial 4/0`
`Router(config-if)#`
	Enter interface configuration mode by specifying the serial interface that you want to configure using the **interface serial** global configuration command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  load-interval  Specify interval for load calculation for an interface`
`  locaddr-priority  Assign a priority group`
`  logging  Configure logging for interface`
`  loopback  Configure internal loopback on an interface`
`  mac-address  Manually set interface MAC address`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface Maximum Transmission Unit (MTU)`
`  netbios  Use a defined NETBIOS access list or enable name-caching`
`  no  Negate a command or set its defaults`
`  nrzi-encoding  Enable use of NRZI encoding`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	Enter **?** to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.

`Router(config-if)# ip ?`
`Interface IP configuration subcommands:`
`  access-group  Specify access control for packets`
`  accounting  Enable IP accounting on this interface`
`  address  Set the IP address of an interface`
`  authentication  authentication subcommands`
`  bandwidth-percent  Set EIGRP bandwidth limit`
`  broadcast-address  Set the broadcast address of an interface`
`  cgmp  Enable/disable CGMP`
`  directed-broadcast  Enable forwarding of directed broadcasts`
`  dvmrp  DVMRP interface commands`
`  hello-interval  Configures IP-EIGRP hello interval`
`  helper-address  Specify a destination address for UDP broadcasts`
`  hold-time  Configures IP-EIGRP hold time`
`  .`
`  .`
`  .`
`Router(config-if)# ip`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ip address ?`
`  A.B.C.D  IP address`
`  negotiated  IP Address negotiated over PPP`
`Router(config-if)# ip address`
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.
	A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 ?`
`  A.B.C.D  IP subnet mask`
`Router(config-if)# ip address 172.16.0.1`
	Enter the keyword or argument you want to use. This example uses the 172.16.0.1 IP address.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.
	A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?`
`  secondary  Make this IP address a secondary address`
`  <cr>`
`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
	Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**.
	A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0` `Router(config-if)#`	In this example, Enter is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands also can have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and

have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A Flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Filtering Output from the show and more Commands

In Cisco IOS Release 12.0(1)T and later releases, you can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

command **|** {**begin | include | exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
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
```

For more information on the search and filter functionality, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Identifying Supported Platforms

Cisco IOS software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS software image, see the following sections:

- Using Feature Navigator
- Using Software Release Notes

Using Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

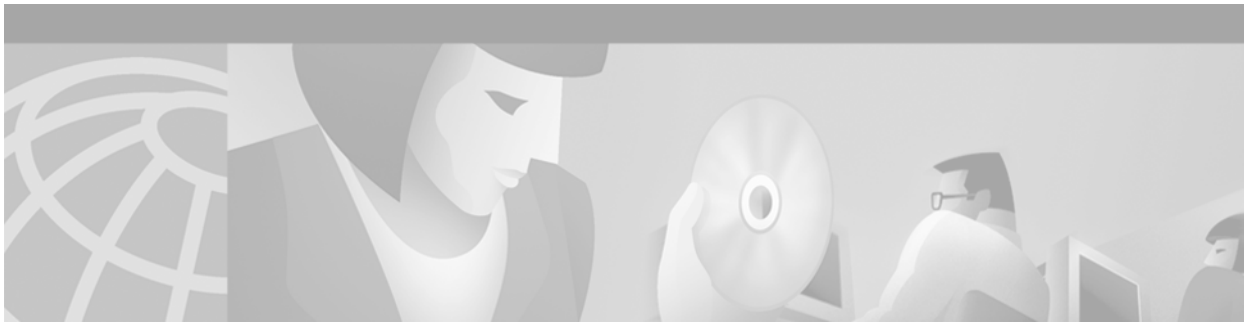
http://www.cisco.com/go/fn

Using Software Release Notes

Cisco IOS software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- Microcode support information
- Feature set tables
- Feature descriptions
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases.



Cisco IOS Switching Commands

This book describes the basic commands used to configure switching features in Cisco IOS software. Refer to the configuration chapter indicated here for configuration guidelines:

For guidelines about configuring this switching feature...	Refer to the following chapters in the *Cisco IOS Switching Services Configuration Guide...*
Cisco IOS Switching Paths	• "Switching Paths Overview" chapter • "Configuring Fast Switching" chapter • "Cisco Express Forwarding Overview" chapter • "Configuring Cisco Express Forwarding" chapter
NetFlow	• "NetFlow Overview" chapter • "Configuring NetFlow" chapter
Multiprotocol Label Switching	• "Multiprotocol Label Switching Overview" chapter • "Configuring Multiprotocol Label Switching" chapter
Multilayer Switching	• "Multilayer Switching Overview" chapter • "Configuring IP Multilayer Switching" chapter • "Configuring IP Multicast Multilayer Switching" chapter • "Configuring IPX Multilayer Switching" chapter
Multicast Distributed Switching	• "Configuring Multicast Distributed Switching" chapter

For guidelines about configuring this switching feature...	Refer to the following chapters in the *Cisco IOS Switching Services Configuration Guide*...
Virtual LANs	• "Routing Between Virtual LANs Overview" chapter • "Configuring Routing Between VLANs with Inter-Switch Link Encapsulation" chapter • "Configuring Routing Between VLANs with IEEE 802.10 Encapsulation" chapter • "Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation" chapter
LAN Emulation	• "LAN Emulation Overview" chapter • "Configuring LAN Emulation" chapter • "Configuring Token Ring LAN Emulation" chapter • "Multiprotocol over ATM Overview" chapter • "Configuring the Multiprotocol over ATM Client" chapter • "Configuring the Multiprotocol over ATM Server" chapter • "Configuring Token Ring LAN Emulation for Multiprotocol over ATM" chapter

access-list rate-limit

To configure an access list for use with committed access rate (CAR) policies, use the **access-list rate-limit** global configuration command. To remove the access list from the configuration, use the **no** form of this command.

access-list rate-limit *acl-index* {*precedence* | *mac-address* | *exp* | **mask** *mask*}

no access-list rate-limit *acl-index* {*precedence* | *mac-address* | *exp* | **mask** *mask*}

Syntax Description

acl-index	Specifies the access list number. Classification options are as follows: • For IP precedence, use any number from 1 to 99. • For MAC address, use any number from 100 to 199. • For MPLS experimental field, use any number from 200 to 299.
precedence	Specifies the IP precedence. Valid values are from 0 to 7.
mac-address	Specifies the MAC address.
exp	Specifies the MPLS experimental field. Valid values are from 0 to 7.
mask *mask*	Specifies the mask. Use this option if you want to assign multiple IP precedences or MPLS experimental field values to the same rate-limit access list.

Defaults

No CAR access lists are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.1(5)T	This command now includes an access list based on the MPLS experimental field.

Usage Guidelines

Use this command to classify packets by the specified IP precedence, MAC address, or MPLS experimental field values for a particular CAR access list. You can then apply CAR policies, using the **rate-limit** command, to individual rate-limit access lists causing packets with different IP precedences, MAC addresses, or MPLS experimental field values to be treated differently by the CAR process.

You can specify only one command for each rate-limit access list. If you enter this command multiple times with the same access list number, the new command overwrites the previous command.

Use the **mask** keyword to assign multiple IP precedences or MPLS experimental field values to the same rate-limit list. To ascertain the **mask** value, perform the following steps:

Step 1 Decide which precedences you want to assign to this rate-limit access list.

Step 2 Convert the precedences or MPLS experimental field values into 8-bit numbers with each bit corresponding to one value. For example, an MPLS experimental field value of 0 corresponds to 00000001, 1 corresponds to 00000010, 6 corresponds to 01000000, and 7 corresponds to 10000000.

Step 3 Add the 8-bit numbers for the selected MPLS experimental field values. For example, the mask for MPLS experimental field values 1 and 6 is 01000010.

Step 4 The command expects hexadecimal format. Convert the binary mask into the corresponding hexadecimal number. For example, 01000010 becomes 42. This value is used in the **access-list rate-limit** command. Any packets that have an MPLS experimental field value of 1 or 6 will match this access list.

A mask of FF matches any precedence; a mask of 00 does not match any precedence.

Examples

In the following example, MPLS experimental fields with the value of 7 are assigned to the rate-limit access list 200:

```
router(config)# access-list rate-limit 200 7
```

You can then use the rate-limit access list in a **rate-limit** command so that the rate limit is applied only to packets matching the rate-limit access list:

```
router(config)# interface atm4/0.1 mpls
router(config-if)# rate-limit input access-group rate-limit 200 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
```

Related Commands

Command	Description
rate-limit	Configures CAR and DCAR policies.
show access-list rate-limit	Displays information about rate-limit access lists.

address-family

To enter the address family submode for configuring routing protocols such as BGP, 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 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 and 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.

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 NLRI for the VPNv4 address family using **neighbor activate** and other related commands:

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

The 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 PE and 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 commands enter the address family submode:

```
router bgp 100
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.

append-after

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

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 default behavior or values.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

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

```
Router(config-ip-expl-path)# append-after 5 next-address 3.3.27.3
```

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.

atm-address

To override the control ATM address of an MPC or MPS, use the **atm-address** command in interface configuration mode. To revert to the default address, use the **no** form of this command.

atm-address *atm-address*

no atm-address

Syntax Description

atm-address	Control ATM address.

Defaults

The default is an automatically generated ATM address.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

This command specifies the control ATM address that an MPC or MPS should use when it comes up; that is, when it is associated with a hardware interface.

The **atm-address** command overrides the default operational control address of the MPC or MPS. When this address is deleted (using the **no** form of the command), the MPC or MPS uses an automatically generated address as its control address.

Examples

The following example specifies the ATM address for an MPC:

```
atm-address 47.009181000000061705b7701.00400BFF0011.00
```

The following example specifies the ATM address for an MPS:

```
atm-address 47.009181000000061705C2B01.00E034553024.00
```

bgp default route-target filter

To enable automatic BGP route-target community filtering, use the **bgp default route-target filter** router configuration command. To disable this feature, 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.

Defaults

This command is enabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **bgp default route-target filter** command to control the distribution of 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 CEBGP border edge router.

If you configure the router for BGP route-target community filtering, all received 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 VRFs. This is the desired behavior for a router configured as a 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(config)# router bgp 120
Router(config-router)# no bgp default route-target filter
```

Related Commands

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

bgp scan-time

To configure scanning intervals of 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	Specifies 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.

Defaults

The default scanning interval is 60 seconds.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
12.07(T)	This command was introduced.

Usage Guidelines

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

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

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.

cable bundle

To configure a cable interface to belong to an interface bundle, use the **cable bundle** interface configuration command. To delete a cable interface bundle definition, use the **no** form of this command.

cable bundle *n* [**master**]

no cable bundle *n* [**master**]

Syntax Description

n	Specifies the bundle identifier. Valid range is from 1 to 255.
master	(Optional) Defines the specified interface as the master.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.

Usage Guidelines

You can configure up to four interface bundles. In each bundle, specify one interface as the master interface by using the optional **master** keyword.

Configure only an IP address on the master interface. If an IP address is configured and the interface is not specified as the master interface, any attempt to add an interface to a bundle is rejected.

Specify all generic IP networking information (such as IP address, routing protocols, and switching modes) on the bundle master interface. Do not specify generic IP networking information on bundle slave interfaces.

If you attempt to add an interface to a bundle as nonmaster interface and an IP address is assigned to this interface, the command will fail. You must remove the IP address configuration before you can add the interface to a bundle.

If you have configured an IP address on a bundled interface and the interface is not the master interface, a warning message appears.

Specify generic (not downstream or upstream related) cable interface configurations, such as source-verify or Address Resolution Protocol (ARP) handling, on the master interface. Do not specify generic configuration on nonmaster interfaces.

If you configure an interface as a part of a bundle and it is not the master interface, all generic cable configuration for this interface is removed. The master interface configuration will then apply to all interfaces in the bundle.

If you shut down or remove the master interface in a bundle, no data packets are sent to any of the interfaces in this bundle. Packets are still physically received from nonmaster interfaces that have not been shut down, but those packets will be discarded. This means that modems connected to those interfaces will not be disconnected immediately, but modems going online will not be able to obtain an IP address, download their configuration file, or renew their IP address assignment if the DHCP lease expires.

If you shut down a slave interface, only this shut down interface is affected.

Examples

The following example configures interface 25 to be the master interface:

```
Router(config-if)# cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up
```

The following example shows the error message that appears if you try to configure an interface with an IP address that is not the master interface:

```
Router(config-if)# cable bundle 5
Please remove ip address config first then reenter this command
```

Related Commands

Command	Description
show cable bundle	Displays the forwarding table for the specified interface bundle.

cable helper-address

To specify a destination address for User Datagram Protocol (UDP) broadcast (DHCP) packets, use the **cable helper-address** interface configuration command.To disable this feature, use the **no** form of this command.

cable helper-address *ip-address* {**cable-modem | host**}

no cable helper-address *ip-address* {**cable-modem | host**}

Syntax Description

ip-address	The IP address of a DHCP server. Based on whether you add the **host** or **cable-modem** keyword at the end of the **cable helper-address** command, it is the IP address of the MSOs CNR server or the ISPs DHCP server.
cable-modem	Specifies that only cable modem UDP broadcasts are forwarded
host	Specifies that only host UDP broadcasts are forwarded.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
11.3 NA	This command was introduced.

Usage Guidelines

If you specify a secondary interface address, the giaddr field in the DHCP requests will be sent to the primary address for DHCP requests received from cable modems, and to the secondary IP address for DHCP requests received from hosts.

Examples

The following example forwards UDP broadcasts from cable modems to the DHCP server at 172.23.66.44:

```
Router(config-if)# cable helper-address 172.23.66.44 cable-modem
```

The following example forwards UDP broadcasts from hosts to the DHCP server at 172.23.66.44:

```
Router(config-if)# cable helper-address 172.23.66.44 host
```

cache

To configure aggregation cache operational parameters, use the **cache** command in aggregation cache configuration mode. To disable the operational parameters, use the **no** form of this command.

cache {**entries** *number* | **timeout** [**active** *minutes* | **inactive** *seconds*]}

no cache {**entries** | **timeout** {**active** | **inactive** }}

Syntax Description

entries *number*	The number of cached entries allowed in the aggregation cache. The number of entries can be 1024 to 524288. The default is 4096.
timeout	Dissolves the session in the aggregation cache.
active *minutes*	(Optional) The number of minutes that an active entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
inactive *seconds*	(Optional) The number of seconds that an inactive entry will stay in the aggregation cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

Defaults

The default for cache entries is 4096.

The default for active cache entries is 30 minutes.

The default for inactive cache entries is 15 seconds.

Command Modes

Aggregation cache configuration

Command History

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

Examples

The following example shows how to set the aggregation cache entry limits:

```
cache entries 2046
cache timeout inactive 199
```

Related Commands

Command	Description
default-name	Enables an aggregation cache.
ip cache-invalidate-delay	Enables the exporting of information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables aggregation cache configuration mode.
show ip cache flow aggregation	Displays the aggregation cache configuration.
show mpoa client	Displays the statistics for the data export, including the main cache and all other enabled caches.

class (MPLS)

To configure a defined MPLS CoS map that specifies how classes map to label VCs (LVCs) when combined with a prefix map, use the **class** command in CoS map submode. To disable this option, 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

No default behavior or values.

Command Modes

CoS map submode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following commands configure a CoS map:

```
tag-switching cos-map 55
class 1 premium
exit
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
show tag-switching cos-map	Displays the CoS map used to assign quantity of LVCs and associated CoS of those LVCs.
tag-switching cos-map	Creates a class map that specifies how classes map to LVCs when combined with a prefix map.
tag-switching prefix-map	Displays the prefix map used to assign a CoS map to network prefixes matching a standard IP access list.

clear adjacency

To clear the Cisco Express Forwarding (CEF) adjacency table, use the **clear adjacency** command in EXEC mode.

clear adjacency

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.

Usage Guidelines

When you issue this command, entries in the adjacency table that reside on the Route Processor (RP) are removed and then adjacency sources (such as ARP and Frame Relay) are requested to repopulate the adjacency tables once again. Layer 2 next hop information is reevaluated.

With distributed CEF (dCEF) mode, the adjacency tables that reside on line cards are always synchronized to the adjacency table that resides on the RP. Therefore, clearing the adjacency table on the RP using the **clear adjacency** command also clears the adjacency tables on the line cards; all changes are propagated to the line cards.

Clearing adjacencies cause the adjacency table to repopulate from the Layer 2 to Layer 3 mapping tables, such as ARP. To cause the mappings to be re-evaluated, the source information must be cleared by using a Cisco IOS command, such as the **clear arp-cache** command.

Examples

The following example clears the adjacency table:

```
Router# clear adjacency
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show adjacency	Displays CEF adjacency table information.

clear atm vc

To release a specified switched virtual circuit (SVC), use the **clear atm vc** command in EXEC mode.

clear atm vc *vcd*

Syntax Description

vcd	Virtual channel descriptor of the channel to be released.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

For multicast or control VCCs, this command causes the LANE client to exit and rejoin an emulated LAN.

For data VCCs, this command also removes the associated LAN Emulation Address Resolution Protocol (LE ARP) table entries.

Examples

The following example releases SVC 1024:

```
clear atm vc 1024
```

clear cef interface

To clear the Cisco Express Forwarding (CEF) per-interface traffic policy statistics for an interface, use the **clear cef interface policy-statistics** command in privileged EXEC mode.

clear cef interface [*interface-type interface-number*] **policy-statistics**

Syntax Description

interface-type	Type of interface to clear the policy statistics for
interface-number	Port, connector, or interface card number

Defaults

If you do not specify an interface type and interface number the policy statistics for all interfaces are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(9)S	This command was introduced to support the Cisco 12000 series Internet routers.
12.0(17)ST	This command was introduced to support the Cisco 12000 series Internet routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command clears the CEF BGP traffic policy statistics counters for an interface.

Examples

The following example clears the CEF BGP traffic policy statistics counters:

```
R1# clear cef interface ethernet 0/0 policy-statistics
R1#
```

Related Commands

Command	Description
bgp-policy	Enables Border Gateway Protocol (BGP) policy accounting or policy propagation on an interface.
show cef interface policy-statistics	Displays detailed Cisco Express Forwarding (CEF) policy statistical information for all interfaces.

clear cef linecard

To clear Cisco Express Forwarding (CEF) information from line cards, use the **clear cef linecard** command in EXEC mode.

clear cef linecard [*slot-number*] [**adjacency** | **interface** | **prefix**]

Syntax Description

slot-number	(Optional) Line card slot number to clear. When you omit this argument, all line card slots are cleared.
adjacency	(Optional) Clears line card adjacency tables and rebuilds adjacency for the specified line card.
interface	(Optional) Clears line card interface information and recreates the interface information for the specified line card.
prefix	(Optional) Clears line card prefix tables and starts rebuilding the forwarding information base (FIB) table.

Command Modes

EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.

Usage Guidelines

This command is available only on distributed switching platforms running dCEF.

CEF information on the line cards is cleared, however, CEF information on the Route Processor (RP) is not affected.

Once you clear CEF information from line cards, the corresponding information from the RP is propagated to the line cards. Interprocess communications (IPC) ensures that CEF information on the RP matches the CEF information on the line cards.

Examples

The following example clears the CEF information from the line cards:

```
clear cef linecard
```

Related Commands

Command	Description
show cef linecard	Displays CEF-related interface information by line card.

clear ip cache

To delete entries in the routing table cache used to fast switch IP traffic, use the **clear ip cache** command in the privileged EXEC mode.

clear ip cache [*prefix mask*]

Syntax Description

prefix mask	(Optional) Deletes only the entries in the cache that match the prefix and mask combination.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to clear routes from the routing table cache. You can remove all entries in the routing cache or you can remove only those entries associated with a specified prefix and mask.

Examples

The following command shows how to delete entire in the routing table cache:

```
Router# clear ip cache
```

The following command show how to delete entries in the router table associated with the prefix and mask 192.168.32.0 255.255.255.0:

```
Router# clear ip cache 192.168.32.0 255.255.255.0
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
show ip cache	Displays the routing table cache used to fast switch IP traffic.

clear ip cef event-log

To clear the Cisco Express Forwarding (CEF) event-log buffer, use the **clear ip cef event-log** command in EXEC mode.

clear ip cef event-log

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command clears the entire CEF table event log that holds forwarding information base (FIB) and adjacency events.

Examples

The following example clears the CEF event-log buffer:

```
Router# clear ip cef event-log
```

Related Commands

Command	Description
IP cef table consistency-check	Enables CEF table consistency checker types and parameters.
ip cef table event-log	Controls CEF table event-log characteristics.
show ip cef events	Displays all recorded CEF FIB and adjacency events.

clear ip cef inconsistency

To clear the Cisco Express Forwarding (CEF) inconsistency statistics and records found by the CEF consistency checkers, use the **clear ip cef inconsistency** command in EXEC mode.

clear ip cef inconsistency

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command clears the CEF inconsistency checker statistics and records that accumulate when the **ip cef table consistency-check** command is enabled.

Examples

The following example clears all CEF inconsistency checker statistics and records:

```
Router# clear ip cef inconsistency
```

Related Commands

Command	Description
ip cef table consistency-check	Enables CEF table consistency checker types and parameters.
show ip cef inconsistency	Displays CEF IP prefix inconsistencies.

clear ip cef prefix-statistics

To clear Cisco Express Forwarding (CEF) counters by resetting the packet and byte count to zero (0), use the **clear ip cef prefix-statistics** command in EXEC mode.

clear ip cef {*network* [*mask*] | *****} **prefix-statistics**

Syntax Description

network	Clears counters for a forwarding information base (FIB) entry specified by network.
mask	(Optional) Clears counters for a FIB entry specified by network and mask.
*	Clears counters for all FIB entries.

Command Modes

EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.

Usage Guidelines

When the clear statistics flag is set, statistics are cleared as the FIB table is scanned. The time period is up to 60 seconds for all statistics to clear. However, clearing a specific prefix is completed immediately.

Examples

The following example resets the packet and byte counts to zero for all CEF entries:

```
clear ip cef * prefix-statistics
```

Related Commands

Command	Description
ip cef accounting	Enables CEF network accounting.
show adjacency	Displays CEF adjacency table information.
show ip cef	Displays entries or a summary of the FIB table.

clear ip flow stats

To clear the NetFlow accounting statistics, use the **clear ip flow stats** command in privileged EXEC mode.

clear ip flow stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CA	This command was introduced.

Usage Guidelines

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

The **show ip cache flow** command displays the NetFlow accounting statistics. Use the **clear ip flow stats** command to clear the NetFlow accounting statistics.

Examples

The following example shows how to clear the NetFlow accounting statistics on the router:

```
Router# clear ip flow stats
```

Related Commands

Command	Description
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 on interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.

clear ip mds

To clear multicast distributed switching (MDS) information from the router, use the **clear ip mds** command in privileged EXEC mode.

clear ip mds {**all** | [**vrf** *vrf-name*] **forwarding**}

Syntax Description

all	(Optional) Clear all IP MDS information.
vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
forwarding	(Optional) Clears all linecard routes from a Multicast Forwarding Information Base (MFIB) table and resynchronizes it with the Route Processor (RP).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.

Usage Guidelines

Cisco 12000 Series Internet Router

On a Cisco 12000 Series Internet Router the **clear ip mds** command must be run in privileged EXEC mode on a linecard.

Examples

The following example clears all line card routes in an MFIB table on a Cisco 12000 Series Internet Router:

```
Router# attach 1
LC-Slot1> enable
LC-Slot1# clear ip mds forwarding
```

```
The following example clears all line card routes in an MFIB table on a Cisco 7500 Series
Router:
Router# clear ip mds forwarding
```

Related Commands

Command	Description
show ip mds interface	Displays the MFIB table and forwarding information for MDS on a line card.
show ip mds stats	Display switching statistics or line card statistics for MDS.
show ip mds summary	Displays a summary of the MFIB table for MDS.
show ip mds forwarding	Displays MDS information for all the interfaces on the line card.

clear ip mds linecard

To reset multicast distributed switching (MDS) line card information on the router, use the **clear ip mds linecard** command in privileged EXEC mode.

clear ip mds linecard {*linecard-slot-number* | *****}

Syntax Description

linecard-slot-number	Slot number containing the line card to be reset.
*	Indicates that the reset should be executed on all line cards.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(19.3)S	This command was introduced.

Usage Guidelines

When the ***** keyword is specified instead of the *linecard-slot-number* argument, all MDS information on all line cards is cleared and reset.

Examples

The following example clears and resets all MDS line card information on the router:

```
Router# clear ip mds linecard *
```

Related Commands

Command	Description
show ip mds	Clears MDS information from the router.
show ip mds interface	Displays the MFIB table and forwarding information for MDS on a line card.
show ip mds stats	Display switching statistics or line card statistics for MDS.
show ip mds summary	Displays a summary of the MFIB table for MDS.
show ip mds forwarding	Displays MDS information for all the interfaces on the line card.

clear ip mds forwarding

The **forwarding** keyword for the **clear ip mds** command is no longer documented as a separate command.

The information for using the **forwarding** keyword for the **clear ip mds** command has been incorporated into the **clear ip mds** command documentation. See the **clear ip mds** command documentation for more information.

clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** command in EXEC mode.

clear ip mroute {***** | *group* [*source*]}

Syntax Description

*****	Deletes all entries from the IP multicast routing table.
group	Either of the following: • Name of the multicast group, as defined in the DNS hosts table or with the **ip host** command. • IP address of the multicast group. This is a multicast IP address in four-part, dotted notation.
source	(Optional) If you specify a group name or address, you can also specify a name or address of a multicast source that is sending to the group. A source need not be a member of the group.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5) T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using this command now clears both the multicast routing table on the MMLS-RP and all multicast MLS cache entries for all MMLS-SEs that are performing multicast MLS for the MMLS-RP. That is, the original clearing occurs, and the derived hardware switching table is also cleared.

Examples

The following example deletes all entries from the IP multicast routing table:

```
clear ip mroute *
```

The following example deletes from the IP multicast routing table all sources on the 10.3.0.0 subnet that are sending to the multicast group 224.2.205.42. Note that this example deletes all sources on network 10.3, not individual sources.

```
clear ip mroute 224.2.205.42 10.3.0.0
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.
show ip mroute	Displays the contents of the IP multicast routing table.

clear ip pim interface count

To clear all line card counts or packet counts, use the **clear ip pim interface count** command in EXEC mode.

clear ip pim interface count

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.

Usage Guidelines

Use this command on a Router Processor (RP) to delete all multicast distributed switching (MDS) statistics for the entire router.

Examples

The following example clears all the line card packets counts:

```
clear ip pim interface count
```

Related Commands

Command	Description
clear ip mds forwarding	Clears all routes from the MFIB table of a line card and resynchronizes it with the RP.

clear ip route vrf

To remove routes from the VRF routing table, use the **clear ip route vrf** command in EXEC mode.

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

Syntax Description

vrf-name	Name of the VPN routing and forwarding instance (VRF) for the static route.
*	Deletes 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.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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 removes the route to the network 10.13.0.0 in the vpn1 routing table:

```
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 lane le-arp

To clear the dynamic LAN Emulation Address Resolution Protocol (LE ARP) table or a single LE ARP entry of the LANE client configured on the specified subinterface or emulated LAN, use the **clear lane le-arp** command in EXEC mode.

Cisco 7500 Series

clear lane le-arp [**interface** *slot/port* [**.***subinterface-number*] | **name** *elan-name*] [**mac-address** *mac-address* | **route-desc segment** *segment-number* **bridge** *bridge-number*]

Cisco 4500 and 4700 Routers

clear lane le-arp [**interface** *number* [**.***subinterface-number*] | **name** *elan-name*] [**mac-address** *mac-address* | **route-desc segment** *segment-number* **bridge** *bridge-number*]

Syntax Description

interface *slot/port*[**.***subinterface-number*]	(Optional) Interface or subinterface for the LANE client whose LE ARP table or entry is to be cleared for the Cisco 7500 series routers. The space between the **interface** keyword and the *slot* argument is optional.
interface *number*[**.***subinterface-number*]	(Optional) Interface or subinterface for the LANE client whose LE ARP table or entry is to be cleared for the Cisco 4500 or 4700 routers. The space between the **interface** keyword and the *number* argument is optional.
name *elan-name*	(Optional) Name of the emulated LAN for the LANE client whose LE ARP table or entry is to be cleared. Maximum length is 32 characters.
mac-address *mac-address*	(Optional) Keyword and MAC address of the LANE client.
route-desc segment *segment-number*	(Optional) Keywords and LANE segment number. The segment number ranges from 1 to 4095.
bridge *bridge-number*	(Optional) Keyword and bridge number that is contained in the route descriptor. The bridge number ranges from 1 to 15.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command removes dynamic LE ARP table entries only. It does not remove static LE ARP table entries.

If you do not specify an interface or an emulated LAN, this command clears all the LE ARP tables of any LANE client in the router.

If you specify a major interface (not a subinterface), this command clears all the LE ARP tables of every LANE client on all the subinterfaces of that interface.

This command also removes the fast-cache entries built from the LE ARP entries.

Examples

The following example clears all the LE ARP tables for all clients on the router:

```
clear lane le-arp
```

The following example clears all the LE ARP tables for all LANE clients on all the subinterfaces of interface 1/0:

```
clear lane le-arp interface 1/0
```

The following example clears the entry corresponding to MAC address 0800.aa00.0101 from the LE ARP table for the LANE client on the emulated LAN named red:

```
clear lane le-arp name red 0800.aa00.0101
```

The following example clears all dynamic entries from the LE ARP table for the LANE client on the emulated LAN named red:

```
clear lane le-arp name red
```

The following example clears the dynamic entry from the LE ARP table for the LANE client on segment number 1, bridge number 1 in the emulated LAN named red:

```
clear lane le-arp name red route-desc segment 1 bridge 1
```

Note MAC addresses are written in the same dotted notation for the **clear lane le-arp** command as they are for the global IP **arp** command.

clear lane server

To force a LANE server to drop a client and allow the LANE configuration server to assign the client to another emulated LAN, use the **clear lane server** command in EXEC mode.

Cisco 7500 Series

clear lane server {**interface** *slot/port* [**.***subinterface-number*] | **name** *elan-name*} [**mac-address** *mac-address* | **client-atm-address** *atm-address* | **lecid** *lane-client-id* | **route-desc segment** *segment-number* **bridge** *bridge-number*]

Cisco 4500 and 4700 Routers

clear lane server {**interface** *number* [**.***subinterface-number*] | **name** *elan-name*} [**mac-address** *mac-address* | **client-atm-address** *atm-address* | **lecid** *lecid* | **route-desc segment** *segment-number* **bridge** *bridge-number*]

Syntax Description

interface *slot/port* [**.***subinterface-number*]	Interface or subinterface where the LANE server is configured for the Cisco 7500 series. The space between the **interface** keyword and the *slot* argument is optional.
interface *number* [**.***subinterface-number*]	Interface or subinterface where the LANE server is configured for the Cisco 4500 or 4700 routers. The space between the **interface** keyword and the *number* argument is optional.
name *elan-name*	Name of the emulated LAN on which the LANE server is configured. Maximum length is 32 characters.
mac-address *mac-address*	(Optional) Keyword and MAC address of the LANE client.
client-atm-address *atm-address*	(Optional) Keyword and ATM address of the LANE client.
lecid *lane-client-id*	(Optional) Keyword and ID of the LANE client. The LANE client ID is a value from 1 to 4096.
route-desc segment *segment-number*	(Optional) Keywords and LANE segment number. The segment number ranges from 1 to 4095.
bridge *bridge-number*	(Optional) Keyword and bridge number that is contained in the route descriptor. The bridge number ranges from 1 to 15.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

After changing the bindings on the configuration server, use this command on the LANE server to force the client to leave one emulated LAN. The LANE server will drop the Control Direct and Control Distribute VCCs to the LANE client. The client will then ask the LANE configuration server for the location of the LANE server of the emulated LAN it should join.

If no LANE client is specified, all LANE clients attached to the LANE server are dropped.

Examples

The following example forces all the LANE clients on the emulated LAN named red to be dropped. The next time they try to join, they will be forced to join a different emulated LAN.

```
clear lane server name red
```

Related Commands

Command	Description
client-atm-address name	Adds a LANE client address entry to the configuration database of the configuration server.
lane database	Creates a named configuration database that can be associated with a configuration server.
mac-address	Sets the MAC layer address of the Cisco Token Ring.
show lane server	Displays global information for the LANE server configured on an interface, on any of its subinterfaces, on a specified subinterface, or on an ELAN.

clear mpoa client cache

To clear the ingress and egress cache entries of one or all MPCs, use the **clear mpoa client cache** command in EXEC mode.

clear mpoa client [**name** *mpc-name*] **cache** [**ingress** | **egress**] [**ip-address** *ip-address*]

Syntax Description

name *mpc-name*	(Optional) Specifies the name of the MPC with the specified name.
ingress	(Optional) Clears ingress cache entries associated with the MPC.
egress	(Optional) Clears egress cache entries associated with the MPC.
ip-address *ip-address*	(Optional) Clears matching cache entries with the specified IP address.

Defaults

The system defaults are:

- All MPC cache entries are cleared.
- Both caches are cleared.
- Entries matching only the specified destination IP address are cleared.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Examples

The following example clears the ingress and egress cache entries for the MPC named ip_mpc:

```
clear mpoa client name ip_mpc cache
```

Related Commands

Command	Description
show mpoa client cache	Displays the ingress or egress cache entries matching the IP addresses for the MPCs.

clear mpoa server cache

To clear the ingress and egress cache entries, use the **clear mpoa server cache** command in EXEC mode.

clear mpoa server [**name** *mps-name*] **cache** [**ingress** | **egress**] [**ip-address** *ip-address*]

Syntax Description

name *mps-name*	(Optional) Specifies the name of the MPS. If this keyword is omitted, this command will apply to all servers.
ingress	(Optional) Clears ingress cache entries associated with a server.
egress	(Optional) Clears egress cache entries associated with a server.
ip-address *ip-address*	(Optional) Clears matching cache entries with the specified IP address. If this keyword is omitted, this command will clear all entries.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

This command clears cache entries.

Examples

The following example clears all cache entries:

```
clear mpoa server cache
```

Related Commands

Command	Description
show mpoa server cache	Displays ingress and egress cache entries associated with a server.

clear vlan

To delete an existing virtual LAN (VLAN) from a management domain, use the **clear vlan** command in privileged EXEC mode.

clear vlan *vlan*

Syntax Description

vlan	Number of the VLAN. Valid values are 2 to 1000.

Command Modes

Privileged EXEC

Usage Guidelines

Follow these guidelines for deleting VLANs:

- When you delete an Ethernet VLAN in Virtual Terminal Protocol (VTP) server mode, the VLAN is removed from all switches in the same VTP domain.
- When you delete a VLAN in VTP transparent mode, the VLAN is deleted only on the current switch.
- To delete a Token Ring Bridge Relay Function (TRBRF) VLAN, you must either first reassign its child Token Ring Concentrator Relay Functions (TRCRFs) to another parent TRBRF or delete the child TRCRFs.

Caution When you clear a VLAN, all ports assigned to that VLAN become inactive. However, the VLAN port assignments are retained until you move the ports to another VLAN. If the cleared VLAN is reactivated, all ports still configured on that VLAN are also reactivated. A warning is displayed if you clear a VLAN that exists in the mapping table.

Examples

The following example shows how to clear an existing VLAN (VLAN 4) from a management domain:

```
Router# clear vlan 4
This command will deactivate all ports on vlan 4
in the entire management domain
Do you want to continue(y/n) [n]? y
VLAN 4 deleted
```

Related Commands

Command	Description
set vlan	Groups ports into a VLAN.
show vlans	Displays VLAN subinterfaces.

clear vlan mapping

To delete existing 802.1Q virtual LAN (VLAN) to Inter-Switch Link (ISL) VLAN-mapped pairs, use the **clear vlan mapping** command in privileged EXEC mode.

clear vlan mapping dot1q {*1q-vlan* | **all**}

Syntax Description

dot1q	Specifies the 802.1Q VLAN.
1q-vlan	Number of the 802.1Q VLAN for which to remove the mapping.
all	Clears the mapping table of all entries.

Command Modes

Privileged EXEC

Examples

The following example shows how to clear an existing mapped 802.1Q VLAN (VLAN 1044) from the mapping table:

```
Router# clear vlan mapping dot1q 1044
Vlan Mapping 1044 Deleted.
```

The following example shows how to clear all mapped 802.1Q VLANs from the mapping table:

```
Router# clear vlan mapping dot1q all
All Vlan Mapping Deleted.
```

Related Commands

Command	Description
set vlan mapping	Maps 802.1Q VLANs to ISL VLANs.
show vlan mapping	Displays VLAN mapping table information.

client-atm-address name

To add a LANE client address entry to the configuration server's configuration database, use the **client-atm-address name** database configuration command. To remove a client address entry from the table, use the **no** form of this command.

client-atm-address *atm-address-template* **name** *elan-name*

no client-atm-address *atm-address-template*

Syntax Description

atm-address-template	Template that explicitly specifies an ATM address or a specific part of an ATM address and uses wildcard characters for other parts of the ATM address, making it easy and convenient to specify multiple addresses matching the explicitly specified part. Wildcard characters can replace any nibble or group of nibbles in the prefix, the end-system identifier (ESI), or the selector fields of the ATM address.
elan-name	Name of the emulated LAN. Maximum length is 32 characters.

Defaults

No address and no emulated LAN name are provided.

Command Modes

Database configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

The effect of this command is to bind any client whose address matches the specified template into the specified emulated LAN. When a client comes up, it consults the LANE configuration server, which responds with the ATM address of the LANE server for the emulated LAN. The client then initiates join procedures with the LANE server.

Before this command is used, the emulated LAN specified by the *elan-name* argument must have been created in the configuration server's database by use of the **name server-atm-address** command.

If an existing entry in the configuration server's database binds the LANE client ATM address to a different emulated LAN, the new command is rejected.

This command affects only the bindings in the named configuration server database. It has no effect on the LANE components themselves.

See the **lane database** command for information about creating the database, and the **name server-atm-address** command for information about binding the emulated LAN's name to the server's ATM address.

The **client-atm-address name** command is a subcommand of the global **lane database** command.

ATM Addresses

A LANE ATM address has the same syntax as a network service access point (NSAP), but it is not a network-level address. It consists of the following:

- A 13-byte prefix that includes the following fields defined by the ATM Forum:
  - AFI (Authority and Format Identifier) field (1 byte), DCC (Data Country Code) or ICD (International Code Designator) field (2 bytes), DFI field (Domain Specific Part Format Identifier) (1 byte), Administrative Authority field (3 bytes), Reserved field (2 bytes), Routing Domain field (2 bytes), and the Area field (2 bytes)
- A 6-byte ESI
- A 1-byte selector field

Address Templates

LANE ATM address templates can use two types of wildcards: an asterisk (*) to match any single character (nibble), and an ellipsis (...) to match any number of leading, middle, or trailing characters. The values of the characters replaced by wildcards come from the automatically assigned ATM address.

In LANE, a *prefix template* explicitly matches the prefix but uses wildcards for the ESI and selector fields. An *ESI template* explicitly matches the ESI field but uses wildcards for the prefix and selector.

In our implementation of LANE, the prefix corresponds to the switch, the ESI corresponds to the ATM interface, and the selector field corresponds to the specific subinterface of the interface.

Examples

The following example uses an ESI template to specify the part of the ATM address corresponding to the interface. This example allows any client on any subinterface of the interface that corresponds to the displayed ESI value, no matter to which switch the router is connected, to join the engineering emulated LAN:

```
client-atm-address ...0800.200C.1001.** name engineering
```

The following example uses a prefix template to specify the part of the ATM address corresponding to the switch. This example allows any client on a subinterface of any interface connected to the switch that corresponds to the displayed prefix to join the marketing emulated LAN:

```
client-atm-address 47.000014155551212f.00.00... name marketing
```

Related Commands

Command	Description
default-name	Provides an ELAN name in the database of the configuration server for those client MAC addresses and client ATM addresses that do not have explicit ELAN name bindings.
lane database	Creates a named configuration database that can be associated with a configuration server.
mac-address	Sets the MAC layer address of the Cisco Token Ring.
name server-atm-address	Specifies or replaces the ATM address of the LANE server for the ELAN in the configuration database of the configuration server.

default-name

To provide an emulated LAN name in the configuration server's database for those client MAC addresses and client ATM addresses that do not have explicit emulated LAN name bindings, use the **default-name** command in database configuration mode. To remove the default name, use the **no** form of this command.

default-name *elan-name*

no default-name

Syntax Description

elan-name	Default emulated LAN name for any LANE client MAC address or LANE client ATM address not explicitly bound to any emulated LAN name. Maximum length is 32 characters.

Defaults

No name is provided.

Command Modes

Database configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command affects only the bindings in the configuration server's database. It has no effect on the LANE components themselves.

The named emulated LAN must already exist in the configuration server's database before this command is used. If the default name-to-emulated LAN name binding already exists, the new binding replaces it.

The **default-name** command is a subcommand of the global **lane database** global configuration command.

Examples

The following example specifies the emulated Token Ring LAN named man as the default emulated LAN. Because none of the emulated LANs are restricted, clients are assigned to whichever emulated LAN they request. Clients that do not request a particular emulated LAN will be assigned to the named man emulated LAN.

```
lane database example2
 name eng server-atm-address 39.000001415555121101020304.0800.200c.1001.02
 name eng local-seg-id 1000
 name man server-atm-address 39.000001415555121101020304.0800.200c.1001.01
 name man local-seg-id 2000
 name mkt server-atm-address 39.000001415555121101020304.0800.200c.4001.01
 name mkt local-seg-id 3000
 default-name man
```

Related Commands

Command	Description
client-atm-address name	Adds a LANE client address entry to the configuration database of the configuration server.
lane database	Creates a named configuration database that can be associated with a configuration server.
mac-address	Sets the MAC layer address of the Cisco Token Ring.
name server-atm-address	Specifies or replaces the ATM address of the LANE server for the ELAN in the configuration database of the configuration server.

enabled (aggregation cache)

To enable a NetFlow accounting aggregation cache, use the **enabled** command in NetFlow aggregation cache configuration mode. To disable a NetFlow accounting aggregation cache, use the **no** form of this command.

enabled

no enabled

Syntax Description

This command has no arguments or keywords.

Defaults

No aggregation cache is enabled.

Command Modes

NetFlow aggregation cache configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable a NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# enabled
```

The following example shows how to disable a NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# no enabled
```

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.

Command	Description
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 on interfaces.

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs (VLANs), use the **encapsulation dot1q** subinterface configuration command.

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

Syntax Description

vlan-id	Virtual LAN identifier. The allowed range is from 1 to 4095.
native	(Optional) Sets the PVID value of the port to the *vlan-id* value.

Defaults

No default values or behaviors.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The **native** keyword was added.

Usage Guidelines

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.

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

Examples

The following example encapsulates VLAN traffic using the IEEE 802.1Q protocol for VLAN 100:

```
interface fastethernet 4/1.100
  encapsulation dot1q 100
```

Related Commands

Command	Description
encapsulation isl	Enables the ISL, 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.

encapsulation isl

To enable the Inter-Switch Link (ISL), use the **encapsulation isl** command in subinterface configuration mode.

encapsulation isl *vlan-identifier*

Syntax Description

vlan-identifier	Virtual LAN (VLAN) identifier. The allowed range is from 1 to 1000.

Defaults

No default values or behaviors.

Command Modes

Subinterface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

ISL is a Cisco protocol for interconnecting multiple switches and routers, and for defining VLAN topologies.

ISL encapsulation is configurable on Fast Ethernet interfaces.

ISL encapsulation adds a 26-byte header to the beginning of the Ethernet frame. The header contains a 10-bit VLAN identifier that conveys VLAN membership identities between switches.

Examples

The following example enables ISL on Fast Ethernet subinterface 2/1.20:

```
interface FastEthernet 2/1.20
 encapsulation isl 400
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
show bridge vlan	Displays virtual LAN subinterfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show vlans	Displays virtual LAN subinterfaces.

encapsulation sde

To enable IEEE 802.10 encapsulation of traffic on a specified subinterface in virtual LANs (VLANs), use the **encapsulation sde** command in subinterface configuration mode. IEEE 802.10 is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

encapsulation sde *said*

Syntax Description

said	Security association identifier. This value is used as the VLAN identifier. The valid range is from 0 to 0xFFFFFFFE.

Defaults

No default values or behaviors.

Command Modes

Subinterface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

SDE encapsulation is configurable only on the following interface types:

IEEE 802.10 Routing	IEEE 802.10 Transparent Bridging
• FDDI	• Ethernet • FDDI • HDLC Serial • Transparent mode • Token Ring

Examples

The following example enables SDE on FDDI subinterface 2/0.1 and assigns a VLAN identifier of 9999:

```
interface fddi 2/0.1
 encapsulation sde 9999
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
show bridge vlan	Displays virtual LAN subinterfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show vlans	Displays virtual LAN subinterfaces.

encapsulation tr-isl trbrf-vlan

To enable TRISL, use the **encapsulation tr-isl trbrf-vlan** command in subinterface configuration mode. TRISL is a Cisco proprietary protocol for interconnecting multiple routers and switches and maintaining VLAN information as traffic goes between switches.

encapsulation tr-isl trbrf-vlan *vlan-id* **bridge-num** *bridge-number*

Syntax Description

vlan-id	Number identifying the VLAN.
bridge-num *bridge-number*	Keyword and specify the identification number of the bridge number on the ISL trunk. Possible values are from 1 to 4095.

Defaults

Disabled

Command Modes

Subinterface configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.

Examples

In the following example, TRISL is enabled on a Fast Ethernet interface:

```
interface FastEthernet4/0.2
 encapsulation tr-isl trbrf-vlan 999 bridge-num 14
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
clear vlan statistics	Removes virtual LAN statistics from any statically or system configured entries.
multiring	Enables collection and use of RIF information.
multiring trcrf-vlan	Creates a pseudo-ring to terminate the RIF for source-routed traffic and assigns it to a VLAN.
show drip	Displays the status of the DRiP database.
show vlans	Displays virtual LAN subinterfaces.
source-bridge trcrf-vlan	Attaches a TrCRF VLAN to the virtual ring of the router.

exit-address-family

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

exit-address-family

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Address family configuration submode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to exit the address family configuration mode:

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

Related Commands

Command	Description
address-family	Enters the address family submode for configuring routing protocols, such as BGP, RIP, and static routing.

export destination

To enable the exporting of information from NetFlow aggregation caches, use the **export destination** command in aggregation cache configuration mode. To disable the exporting of NetFlow aggregation cache information, use the **no** form of this command.

export destination *ip-address port*

no export destination *ip-address port*

Syntax Description

ip-address	Destination IP address.
port	Destination UDP port.

Defaults

An export destination is not set.

Command Modes

Aggregation cache configuration

Command History

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

Usage Guidelines

For version 8 data exports, the maximum number of aggregated flow records and the maximum size in bytes of each UDP datagram are as follows:

Aggregation Scheme	Max. Number of Flow Records	UDP Packet Size
BGP Autonomous System	51	1456 bytes
Destination Prefix	44	1436 bytes
Prefix	35	1428 bytes
Protocol Port	51	1456 bytes
Source Prefix	44	1436 bytes

Examples

The following example shows how to configure an export destination for an aggregation cache:

```
export destination 10.41.41.1 9992
```

Related Commands

Command	Description
clear adjacency	Configures aggregation cache operational parameters.
default-name	Enables an aggregation cache.
ip flow-aggregation cache	Enables aggregation cache configuration mode.
show ip cache flow aggregation	Displays the aggregation cache configuration.
show mpoa client	Displays the statistics for the data export including the main cache and all other enabled caches.

export map

To configure an export route map for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **export map** command in VRF configuration submode. To remove an export route map, use the **no** form of this command.

export map *route-map*

no export map *route-map*

Syntax Description

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

Defaults

This command has no default behavior or values. A VRF has no export map unless one is configured using the **export map** command.

Command Modes

VRF configuration submode

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

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

The **export map** command associates a route map with the specified VRF. You can use a route map to filter target routes for a target VPN export by a VRF, based on the route target extended community attributes of the route. The route map might deny export to selected routes from a community on the export list.

An **export map** command with a **set extcommunity rt** command takes precedence over configured route targets (RTs), unless the **additive** keyword is specified. If the export map has a **set community rt1 rt2 additive** command, the previous RT list is kept and rt1 and rt2 are added to the RT list.

Examples

The following example shows how to configure an export map for VRF vpn1:

```
Router(config)# ip vrf vpn1

Router(config-vrf)# export map export1
```

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
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

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

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 VSI on this interface using the **tag-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 physical descriptor. The *vsi-descriptor* string must match the corresponding VSI physical descriptor.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

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

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 examples show how to create an extended MPLS ATM interface, using different command qualifiers:

The following example creates an extended MPLS ATM interface and binds it to BPX port 2.3:

```
interface XTagATM23
extended-port atm0/0 bpx 2.3
```

The following example creates an extended MPLS ATM interface and binds it to port 2.4:

```
interface XTagATM24
extended-port atm0/0 descriptor 0.2.4.0
```

The following example creates an extended MPLS ATM interface and binds it to port 1622:

```
interface XTagATM1622
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.

holding-time

To specify the holding time value for the MPS-p7 variable of an MPS, use the **holding-time** command in MPS configuration mode. To revert to the default value, use the **no** form of this command.

holding-time *time*

no holding-time *time*

Syntax Description

time	Specifies the holding time value in seconds.

Defaults

The default holding time is 1200 seconds (20 minutes).

Command Modes

MPS configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Examples

The following example sets the holding time to 600 seconds (10 minutes):

```
holding-time 600
```

import map

To configure an import route map for a VRF, 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

There is no default. 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.

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:

```
ip vrf vrf_blue
import map blue_import_map
```

Related Commands

Command	Description
export map	Configures an export map for a VRF.
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** ip explicit path subcommand. To disable this feature, 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. (Currently you can use only the **next-address** command.)

Defaults

No default behavior or values.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the **next-address** command is inserted at index 6:

```
Router(cfg-ip-expl-path)# index 6 next-address 3.3.29.3

Explicit Path identifier 6:
    6: next-address 3.3.29.3
```

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.

interface atm

To enter interface configuration mode, specify ATM as the interface type, and create a subinterface on that interface type, use the **interface atm** global configuration command.

interface atm *interface.subinterface-number* [**mpls | tag-switching | point-to-point | multipoint**]

Syntax Description

interface	Specifies a (physical) ATM interface (for example, 3/0).
.*subinterface-number*	Specifies the subinterface number for the ATM interface. On Cisco 7500 series routers, subinterface numbers can range from 0 to 4294967285.
mpls	(Optional) Specifies MPLS as the interface type for which a subinterface is to be created.
tag-switching	(Optional) Specifies tag switching as the interface type for which a subinterface is to be created.
point-to-point	(Optional) Specifies point-to-point as the interface type for which a subinterface is to be created.
multipoint	(Optional) Specifies multipoint as the interface type for which a subinterface is to be created.

Defaults

This command has no default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	New optional subinterface types were introduced.

Usage Guidelines

The **interface atm** command enables you to define a subinterface for a specified type of ATM interface. The subinterface for the ATM interface is created the first time this command is issued with a specified subinterface number.

Examples

For physical ATM interface 3/0, the following command creates an ATM MPLS subinterface having subinterface number 1:

```
Router# interface atm 3/0.1 mpls
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more MPLS interfaces that have been configured for label switching.

interface fastethernet

To select a particular Fast Ethernet interface for configuration, use the **interface fastethernet** global configuration command.

Cisco 4500 and 4700 Series Routers

interface fastethernet *number*

Cisco 7200 Series Routers

interface fastethernet *slot*/*port*

Cisco 7500 Series Routers

interface fastethernet *slot*/*port-adapter*/*port*

Syntax Description

number	Port, connector, or interface card number. On Cisco 4500 or 4700 series routers, specifies the Network Interface Module (NIM) or Networking Products Marketplace (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
slot	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
port	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
port-adapter	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3	Default encapsulation type was changed to Advanced Research Projects Agency (ARPA).

Usage Guidelines

This command does not have a **no** form.

Examples

The following example configures Fast Ethernet interface 0 for standard ARPA encapsulation (the default setting) on Cisco 4500 or 4700 series routers:

```
interface fastethernet 0
```

Related Commands

Command	Description
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.

interface XTagATM

To enter interface configuration mode for the extended MPLS ATM (XTagATM) interface, use the following **interface XTagATM** global configuration command.

interface XTagATM *if-num*

Syntax Description

if-num	Specifies the interface number.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

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.

The interface is created the first time this command is issued for a particular interface number.

Examples

The following example shows how you create an extended MPLS ATM interface with interface number 62:

```
(config)# interface XTagATM62
```

Related Commands

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

ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** command in global configuration mode. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

ip cache-invalidate-delay [*minimum maximum quiet threshold*]

no ip cache-invalidate-delay

Syntax Description

minimum	(Optional) Minimum time (in seconds) between invalidation request and actual invalidation. The default is 2 seconds.
maximum	(Optional) Maximum time (in seconds) between invalidation request and actual invalidation. The default is 5 seconds.
quiet	(Optional) Length of quiet period (in seconds) before invalidation.
threshold	(Optional) Maximum number of invalidation requests considered to be quiet.

Defaults

minimum: 2 seconds
maximum: 5 seconds, and 3 seconds with no more than zero invalidation requests

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

After you enter the **ip cache-invalidate-delay command** all cache invalidation requests are honored immediately.

Caution This command should only be used under the guidance of technical support personnel. Incorrect settings can seriously degrade network performance. The command-line-interface (CLI) will not allow you to enter the **ip cache-invalidate-delay** command until you configure the **service internal** command in global configuration mode.

The IP fast-switching and autonomous-switching features maintain a cache of IP routes for rapid access. When a packet is to be forwarded and the corresponding route is not present in the cache, the packet is process switched and a new cache entry is built. However, when routing table changes occur (such as when a link or an interface goes down), the route cache must be flushed so that it can be rebuilt with up-to-date routing information.

This command controls how the route cache is flushed. The intent is to delay invalidation of the cache until after routing has settled down. Because route table changes tend to be clustered in a short period of time, and the cache may be flushed repeatedly, a high CPU load might be placed on the router.

When this feature is enabled, and the system requests that the route cache be flushed, the request is held for at least *minimum* seconds. Then the system determines whether the cache has been "quiet" (that is, less than *threshold* invalidation requests in the last *quiet* seconds). If the cache has been quiet, the cache is then flushed. If the cache does not become quiet within *maximum* seconds after the first request, it is flushed unconditionally.

Manipulation of these parameters trades off CPU utilization versus route convergence time. Timing of the routing protocols is not affected, but removal of stale cache entries is affected.

Examples

The following example shows how to set a minimum delay of 5 seconds, a maximum delay of 30 seconds, and a quiet threshold of no more than 5 invalidation requests in the previous 10 seconds:

```
Router(config)# service internal
Router(config)# ip cache-invalidate-delay 5 30 10 5
```

Related Commands

Command	Description
ip route-cache	Configures the high-speed switching caches for IP routing.

ip cef

To enable Cisco Express Forwarding (CEF) on the Route Processor card, use the **ip cef** command in global configuration mode. To disable CEF, use the **no** form of this command.

ip cef [**distributed**]

no ip cef [**distributed**]

Syntax Description

distributed	(Optional) Enables distributed CEF (dCEF) operation. Distributes CEF information to line cards. Line cards perform express forwarding.

Defaults

CEF is disabled by default, excluding these platforms:

CEF is enabled on the Cisco 7100 series router.
CEF is enabled on the Cisco 7200 series router.
CEF is enabled on the Cisco 7500 series Internet router.
Distributed CEF is enabled on the Cisco 6500 series router
Distributed CEF is enabled on the Cisco 12000 series Internet router.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.2	The default for the **ip cef** command on Cisco 7200 series routers was changed from disabled to enabled.

Usage Guidelines

This command is not available on the Cisco 12000 series because that router series operates only in dCEF mode.

CEF is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.

Examples

The following example enables standard CEF operation:

```
ip cef
```

The following example enables dCEF operation:

```
ip cef distributed
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.

ip cef accounting

To enable Cisco Express Forwarding (CEF) network accounting, use the **ip cef accounting** command in global configuration mode or interface configuration mode. To disable network accounting of CEF, use the **no** form of this command.

ip cef accounting {[**non-recursive**] [**per-prefix**] [**prefix-length**]}

no ip cef accounting {[**non-recursive**] [**per-prefix**] [**prefix-length**]}

Specific CEF Accounting Information Through Interface Configuration Mode

ip cef accounting non-recursive {**external | internal**}

no ip cef accounting non-recursive {**external | internal**}

Syntax Description

non-recursive	Enables accounting through nonrecursive prefixes. This keyword is optional when used in global configuration mode.
per-prefix	(Optional) Enables the collection of the number of packets and bytes express forwarded to a destination (or prefix).
prefix-length	(Optional) Enables accounting through prefixlength.
external	Counts input traffic in the nonrecursive external bin.
internal	Counts input traffic in the nonrecursive internal bin.

Defaults

Accounting is disabled by default.

Command Modes

Global configuration

Interface configuration

Command History

Release	Modification
11.2 GS	This command was introduced.
11.1 CC	Multiple platform support was added.
11.1 CC	The **prefix-length** keyword was added.
12.2(2)T	The **ip cef accounting non-recursive** command in interface configuration mode was added.

Usage Guidelines

You might want to collect statistics to better understand CEF patterns in your network.

When you enable network accounting for CEF from global configuration mode, accounting information is collected at the Route Processor (RP) when CEF mode is enabled and at the line cards when distributed CEF (dCEF) mode is enabled. You can then display the collected accounting information using the **show ip cef** EXEC command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables the collection of packets and bytes to be express forwarded through a prefix. This keyword is optional when this command is used in global configuration mode.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ip cef detail** EXEC mode command.

Examples

The following example enables the collection of CEF accounting information:

```
ip cef accounting
```

Related Commands

Command	Description
show ip cef	Displays entries or a summary of the FIB table.

ip cef linecard ipc memory

To configure the line card memory pool for the Cisco Express Forwarding (CEF) queuing messages, use the **ip cef linecard ipc memory** command. To return to the default ipc memory allocation, use the **no** form of this command.

ip cef linecard ipc memory *kbps*

no ip cef linecard ipc memory *kbps*

Syntax Description

kbps	Kilobytes of line card memory allocated. Range is 0 to 12800.

Defaults

Default ipc memory allocation is 25 messages. However, this value is dependant on switching platform.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

This command is available only on distributed switching platforms.

If you are expecting large routing updates to the Route Processor (RP), use this command to allocate a larger memory pool on the line cards for queuing CEF routing update messages. The memory pool reduces the transient memory requirements on the RP.

To display and monitor the current size of the CEF message queues, use the **show cef linecard** command. Also, the peak size is recorded and displayed when you use the **detail** keyword.

Examples

The following example configures the CEF line card memory queue to 128000 kilobytes:

```
Router(config)# ip cef linecard ipc memory 128000
```

Related Commands

Command	Description
show cef linecard	Displays detailed CEF information for the specified line card.

ip cef load-sharing algorithm

To select a Cisco Express Forwarding (CEF) load balancing algorithm, use the **ip cef load-sharing algorithm** command in global configuration mode. To return to the default universal load balancing algorithm, use the **no** form of this command.

ip cef load-sharing algorithm {**original** | **tunnel** [*id*] | **universal** [*id*]}

no ip cef load-sharing algorithm {**original** | **tunnel** [*id*] | **universal** [*id*]}

Syntax Description

original	Sets the load balancing algorithm to the original based on a source and destination hash.
tunnel	Sets the load balancing algorithm for use in tunnel environments or in environments where there are only a few IP source and destination address pairs.
universal	Sets the load balancing algorithm to the universal algorithm that uses a source and destination, and ID hash.
id	(Optional) Fixed identifier.

Defaults

Universal load sharing algorithm.

Command Modes

Global 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.

Usage Guidelines

The original CEF load sharing algorithm produced distortions in load sharing across multiple routers due to the use of the same algorithm on every router. When the load sharing algorithm is set to universal mode, each router on the network can make a different load sharing decision for each source-destination address pair which resolves load sharing distortions.

The tunnel algorithm is designed to more fairly share load when only a few source-destination pairs are involved.

Examples

The following example enables the CEF load sharing algorithm for universal environments:

```
ip cef load-sharing algorithm universal 1
```

Related Commands

Command	Description
debug ip cef hash	Records CEF load sharing hash algorithm events
ip load-sharing	Enables load balancing.

ip cef table adjacency-prefix

To modify how Cisco Express Forwarding (CEF) adjacency prefixes are managed, use the **ip cef table adjacency-prefix** command in global configuration mode. To disable CEF adjacency prefix management, use the **no** form of this command.

ip cef table adjacency-prefix [**override | validate**]

no ip cef table adjacency-prefix [**override | validate**]

Syntax Description

override	Enables Cisco Express Forwarding (CEF) adjacency prefixes to override static host glean routes.
validate	Enables the periodic validation of Cisco Express Forwarding (CEF) adjacency prefixes.

Defaults

All CEF adjacency prefix management is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(16)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.1(13)E07 12.1(19.02)E 12.3(04)XG 12.3(04)XK 12.3(06.01)PI03	The validate keyword was added. The default behavior for **ip cef table adjacency-prefix override** was changed to disabled

Usage Guidelines

When CEF is configured, the forwarding information base (FIB) table may conflict with static host routes that are specified in terms of an output interface or created by a Layer 2 address resolution protocols such as Address Resolution Protocol (ARP), map lists, and so on.

The Layer 2 address resolution protocol adds adjacencies to CEF, which in turn creates a corresponding host route entry in the FIB table. This entry is called an adjacency prefix.

override

If the CEF adjacency prefix entries are also configured by a static host route, a conflict occurs.

This command ensures that adjacency prefixes can override static host glean routes, and correctly restore routes when the adjacency prefix is deleted.

validate

When you add a /31 netmask route, the new netmask does not overwrite an existing /32 CEF entry. This problem is resolved by configuring the **validate** keyword to periodically validate prefixes derived from adjacencies in the FIB against prefixes originating from the RIB.

Examples

override

The following example shows how to enable CEF table adjacency prefix override:

```
Router(config)# ip cef table adjacency-prefix override
```

validate

The following example shows how to enable CEF table adjacency prefix validation:

```
Router(config)# ip cef table adjacency-prefix validate
```

ip cef table adjacency-prefix override

The **override** keyword for the **ip cef table adjacency-prefix** command is no longer documented as a separate command.

The information for using the **override** keyword for the **ip cef table adjacency-prefix** command has been incorporated into the **ip cef table adjacency-prefix** command documentation. See the **ip cef table adjacency-prefix** command documentation for more information.

IP cef table consistency-check

To enable Cisco Express Forwarding (CEF) table consistency checker types and parameters, use the **ip cef table consistency-check** command in global configuration mode. To disable consistency checkers, use the **no** form of this command.

ip cef table consistency-check [**type** {**lc-detect** | **scan-lc** | **scan-rib** | **scan-rp**}] [**count** *count_number*] [**period** *seconds*]

no ip cef table consistency-check [**type** {**lc-detect** | **scan-lc** | **scan-rib** | **scan-rp**}] [**count** *count_number*] [**period** *seconds*]

Specific to Suppress Errors During Route Updates

ip cef table consistency-check [**settle-time** *seconds*]

no ip cef table consistency-check [**settle-time** *seconds*]

Syntax Description

type	(Optional) Type of consistency check to configure.
lc-detect	(Optional) Line card detects missing prefix. Confirmed by Route Processor (RP).
scan-lc	(Optional) Passive scan check of tables on line card.
scan-rib	(Optional) Passive scan check of tables on RP against Routing Information Base (RIB).
scan-rp	(Optional) Passive scan check of tables on RP.
count *count_number*	(Optional) Maximum number of prefixes to check per scan. Range is from 1 to 225.
period *seconds*	(Optional) Period between scans. Range is from 30 to 3600 seconds.
settle-time *seconds*	(Optional) Time elapsed during which updates for a candidate prefix are ignored as inconsistencies. Range is from 1 to 3600 seconds.

Defaults

All consistency checkers are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command configures CEF consistency checkers and parameters for the following detection mechanism types:

Detection Mechanism	Operates On	Description
Lc-detect	Line Card	Operates on the line card by retrieving IP prefixes found missing from its forwarding information base (FIB) table. If IP prefixes are missing, the line card can not forward packets for these addresses. Lc-detect will then send IP prefixes to the RP for confirmation. If the RP detects that it has the relevant entry, an inconsistency is detected and an error message will be displayed. Also, the RP will send a signal back to the line card confirming that the IP prefix is an inconsistency.
Scan-lc	Line Card	Operates on the line card by looking through the FIB table for a configurable time period and sending the next *n* prefixes to the RP. The RP does an exact lookup. If it finds the prefix missing, the RP reports an inconsistency. Finally, the RP sends a signal back to the line card for confirmation.
Scan-rp	Route Processor	Operates on the RP (opposite of the scan-lc) by looking through the FIB table for a configurable time period and sending the next *n* prefixes to the line card. The line card does an exact lookup. If it finds the prefix missing, the line card reports an inconsistency and finally signals the RP for confirmation.
Scan-rib	Route Processor	Operates on all RPs (even nondistributed), and scans the RIBto ensure that prefix entries are present in the RP FIB table.

Examples

The following example enables the CEF consistency checkers:

```
ip cef table consistency-check
```

Related Commands

Command	Description
clear ip cef inconsistency	Clears CEF inconsistency statistics and records found by the CEF consistency checkers.
debug ip cef	Displays various CEF table query and check events.
show ip cef inconsistency	Displays CEF IP prefix inconsistencies.

ip cef table event-log

To control Cisco Express Forwarding (CEF) table event-log characteristics, use the **ip cef table event-log** command in global configuration mode.

ip cef table event-log [**size** *event-number*] [**match** *ip-prefix mask*]

no ip cef table event-log [**size** *event-number*] [**match** *ip-prefix mask*]

Specific to Virtual Private Network (VPN) Event Log

ip cef table event-log [**size** *event-number*] [**vrf** *vrf-name*] [**match** ***ip-prefix mask***]

no ip cef table event-log [**size** *event-number*] [**vrf** *vrf-name*] [**match** ***ip-prefix mask***]

Syntax Description

size *event-number*	(Optional) Number of event entries. The range is from 1 to 4294967295.
match	(Optional) Log events matching specified prefix and mask.
ip-prefix	(Optional) IP prefixes matched, in dotted decimal format (A.B.C.D).
mask	(Optional) Network mask written as A.B.C.D.
vrf *vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) instance CEF table and VRF name.

Defaults

Default size for event log is 10000 entries.

Command Modes

Global configuration

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command is used to troubleshoot inconsistencies that occur in the CEF event log between the routes in the Routing Information Base (RIB), Route Processor (RP) CEF tables and line card CEF tables.

The CEF event log collects CEF events as they occur without debugging enabled. This allows the tracing of an event immediately after it occurs. Cisco technical personnel may ask for information from this event log to aid in resolving problems with the CEF feature.

When the CEF table event log has reached its capacity, the oldest event is written over by the newest event until the event log size is reset using this command or cleared using the **clear ip cef event-log** command.

Examples

The following example sets the CEF table event log size to 5000 entries:

```
ip cef table event-log size 5000
```

Related Commands

Command	Description
IP cef table consistency-check	Enables CEF table consistency checker types and parameters.
show ip cef events	Displays all recorded CEF FIB and adjacency events.
clear ip cef event-log	Clears the CEF event-log buffer.

ip cef table resolution-timer

To change the Cisco Express Forwarding (CEF) background resolution timer, use the **ip cef table resolution-timer** command in global configuration mode.

ip cef table resolution-timer *seconds*

no ip cef table resolution-timer *seconds*

Syntax Description

seconds	Range is from 0 to 30 seconds; 0 is for the automatic exponential backoff scheme.

Defaults

The default configuration value is 0 seconds for automatic exponential backoff.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The CEF background resolution timer can use either a fixed time interval or an exponential backoff timer that reacts to the amount of resolution work required. The exponential backoff timer starts at 1 second, increasing to 16 seconds when a network flap is in progress. When the network recovers, the timer returns to 1 second.

The default is used for the exponential backoff timer. During normal operation, the default configuration value set to 0 results in re-resolution occurring much sooner than when the timer is set at a higher fixed interval.

Examples

The following example sets the CEF background resolution timer to 3 seconds:

```
ip cef table resolution-timer 3
```

ip cef traffic-statistics

To change the time intervals used to control the collection of Cisco Express Forwarding (CEF) traffic load statistics, use the **ip cef traffic-statistics** command in global configuration mode. To restore the default values, use the **no** form of this command.

ip cef traffic-statistics [**load-interval** *seconds*] [**update-rate** *seconds*]

no ip cef traffic-statistics

Syntax Description

load-interval *seconds*	(Optional) The interval time over which the CEF traffic load statistics are calculated. The **load-interval** range is from 30 to 300 seconds, in 30-second increments. The default value is 30 seconds.
update-rate *seconds*	(Optional) Frequency with which the port adapter sends the CEF traffic load statistics to the Router Processor (RP). The default value is 10 seconds.

Defaults

load-interval: 30 seconds

update-rate: 10 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command configures the CEF traffic load statistics that are used to determine the behavior of the Next Hop Resolution Protocol (NHRP) — a protocol used by routers to dynamically discover the MAC address of other routers and hosts connected to a nonbroadcast multiaccess (NBMA) network.

The **ip nhrp trigger-svc** command sets the threshold by which NHRP sets up and tears down a connection. The threshold is the CEF traffic load statistics. To change the interval over which that threshold is determined, use the **load-interval** *seconds* keyword and argument of the **ip cef traffic-statistics** command.

Examples

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
ip cef traffic-statistics load-interval 120
```

Related Commands

Command	Description
ip nhrp trigger-svc	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

ip dhcp relay information option

To enable the system to insert the cable modem MAC address into a DHCP packet received from a cable modem or host and forward the packet to a DHCP server, use the **ip dhcp relay information option** in global configuration mode. To disable MAC address insertion, use the **no** form of this command.

ip dhcp relay information option

no ip dhcp relay information option

Syntax Description

This command has no keywords or arguments.

Defaults

MAC address insertion is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3 NA	This command was introduced.
12.0	In previous releases, routers running Cisco IOS Release 11.3 NA used the **cable relay-agent option** command in the cable interface configuration mode. Cisco uBR7200 series routers running Cisco IOS Release 12.0 use the **ip dhcp relay information option** command in the global configuration mode.
12.0 SC	This command was modified to configure the **cable relay-agent option** using **ip dhcp relay information option**.

Usage Guidelines

This functionality enables a DHCP server to identify the user (cable modem) sending the request and initiate appropriate action based on this information. To insert DHCP relay-agent option fields, use the **cable ip dhcp relay information option** command in global configuration mode.

In Cisco uBR7200 series routers running Cisco IOS Release 12.0, use the **ip dhcp relay information option** global configuration command to insert DHCP relay-agent option fields. Previously, routers running Cisco IOS Release 11.3 NA used the **cable relay-agent-option** command.

Cisco IOS Release 12.0 SC was built off Cisco IOS Release 11.3 NA with additional features such as interface bundling. If you use Cisco Release IOS Release 12.0(7) XR2 for concatenation, you should be able to configure the cable relay agent option using the **ip dhcp relay information option** command.

Examples

The following example enables the insertion of DHCP relay agent information into DHCP packets:

```
interface cable 6/0
cable ip dhcp relay information option
```

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 router 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

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the explicit path command mode for IP explicit paths is entered and a path with the number 500 is created:

```
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-aggregation cache

To enable aggregation cache configuration mode, use the **ip flow-aggregation cache** global configuration command. To disable aggregation cache configuration mode, use the **no** form of this command.

ip flow-aggregation cache {**as** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**}

no ip flow-aggregation cache {**as** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**}

Syntax Description

as	Configures the autonomous system aggregation cache scheme.
destination-prefix	Configures the destination prefix aggregation cache scheme.
prefix	Configures the prefix aggregation cache scheme.
protocol-port	Configures the protocol port aggregation cache scheme.
source-prefix	Configures the source prefix aggregation cache scheme.

Defaults

This command is not enabled by default.

Command Modes

Global configuration

Command History

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

Usage Guidelines

In source-prefix aggregation mode, only the source mask is configurable. In destination-prefix aggregation mode, only the destination mask is configurable.

Examples

The following example shows how to enable an autonomous system aggregation scheme:

```
ip flow-aggregation cache as
enable
```

Related Commands

Command	Description
mask destination	Specifies the destination mask.
mask source	Specifies the source mask.
show ip cache flow aggregation	Displays the aggregation cache configuration.

ip flow-cache entries

To change the number of entries maintained in the NetFlow cache, use the **ip flow-cache entries** command in global configuration mode. To return to the default number of entries, use the **no** form of this command.

ip flow-cache entries *number*

no ip flow-cache entries

Syntax Description

number	Number of entries to maintain in the NetFlow cache. The valid range is from 1024 to 524288 entries. The default is 65536 (64K).

Defaults

65536 entries (64K)

Command Modes

Global configuration

Command History

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

Usage Guidelines

Normally the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the **show ip cache flow** EXEC command.

The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If only a few free flows remain, NetFlow attempts to age 30 flows using an accelerated timeout. If only one free flow remains, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure free flow entries are always available.

Caution We recommend that you do not change the NetFlow cache entries. Improper use of this command could cause network problems. To return to the default NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Examples

The following example increases the number of entries in the NetFlow cache to 131,072 (128K):

```
ip flow-cache entries 131072
```

Related Commands

Command	Description
show mpoa client	Displays the routing table cache used to fast switch IP traffic.

ip flow-export

To enable the exporting of information in NetFlow cache entries, use the **ip flow-export** command in global configuration mode. To disable the exporting of information, use the **no** form of this command.

ip flow-export *ip-address udp-port* [**version 1** | **version 5** [**origin-as** | **peer-as**]]

no ip flow-export

Syntax Description

ip-address	IP address of the workstation to which you want to send the NetFlow information.
udp-port	UDP protocol-specific port number.
version 1	(Optional) Specifies that the export packet uses the version 1 format. This is the default. The version field occupies the first two bytes of the export record. The number of records stored in the datagram is a variable from 1 to 24 for version 1.
version 5	(Optional) Specifies that the export packet uses the version 5 format. The number of records stored in the datagram is a variable between 1 and 30 for version 5.
origin-as	(Optional) Specifies that export statistics include the origin autonomous system (AS) for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer AS for the source and destination.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1 CA	This command was introduced.

Usage Guidelines

There is a lot of information in a NetFlow cache entry. When flow switching is enabled with the **ip route-cache flow** command, you can use the **ip flow-export** command to configure the router to export the flow cache entry to a workstation when a flow expires. This feature can be useful for purposes of statistics, billing, and security.

Version 5 format includes the source and destination AS addresses, source and destination prefix masks, and a sequence number. Because this change may appear on your router as a maintenance release, support for version 1 format is maintained with the **version 1** keyword.

Caution Entering the **ip flow-export** or **no ip flow-export** command on the Cisco 12000 Series Internet Routers and specifying any version format other than version 1 (in other words, entering the **ip flow-export** or **no ip flow-export** command and specifying the **version 5** keyword) causes packet forwarding to stop

for a few seconds while NetFlow reloads the route processor and line card CEF tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.

For more information on version 1 and version 5 data format, refer to the "NetFlow Data Format" section in the "Configuring NetFlow Switching" chapter of the *Cisco IOS Switching Services Configuration Guide*.

Examples

The following example configures the router to export the NetFlow cache entry to UDP port 125 on the workstation at 134.22.23.7 when the flow expires using version 1 format:

```
ip flow-export 134.22.23.7 125
```

The following example configures the router to export the NetFlow cache entry to UDP port 2048 on the workstation at 134.22.23.7 when the flow expires using version 5 format and includes the peer AS information:

```
ip flow-export 134.22.23.7 2048 version 5 peer-as
```

Related Commands

Command	Description
ip route-cache flow	Enables NetFlow switching for IP routing.

ip flow-export source

To specify the source interface IP address used in the NetFlow export datagram, use the **ip flow-export source** command in global configuration mode. To remove the source address, use the **no** form of this command.

ip flow-export source *interface*

no ip flow-export source

Syntax Description

interface	Interface from which the router gets the source IP address for the packet.

Defaults

No source interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CA	This command was introduced.

Usage Guidelines

After you configure NetFlow data export, you can also specify the source interface used in the UDP datagram containing the export data. The NetFlow Collector on the workstation uses the IP address of the source interface to determine which router sent the information. The NetFlow Collector also performs SNMP queries to the router using the IP address of the source interface. Because the IP address of the source interface can change (for example, the interface might flap so a different interface is used to send the data), we recommend you configure a loopback source interface. A loopback interface is always up and can respond to SNMP queries from the NetFlow Collector on the workstation.

Examples

The following example shows the configuration for a loopback source interface. The loopback interface has the IP address 4.0.0.1 and is used by the serial interface in slot 5, port 0.

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 4.0.0.1 255.0.0.0
Router(config-if)# exit
Router(config)# interface serial 5/0:0
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ip route-cache flow
Router(config-if)# exit
Router(config)# ip flow-export source loopback0
Router(config)# exit
```

Related Commands

Command	Description
ip flow-cache	Enables the exporting of information in NetFlow cache entries.

ip load-sharing

To enable load balancing for Cisco Express Forwarding (CEF), use the **ip load-sharing** command in interface configuration mode.

ip load-sharing [**per-packet**] [**per-destination**]

Syntax Description

per-packet	(Optional) Enables per-packet load balancing on the interface.
per-destination	(Optional) Enables per-destination load balancing on the interface.

Defaults

Per-destination load balancing is enabled by default when you enable CEF.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 GS	This command was introduced.
11.1 CC	Multiple platform support was added.

Usage Guidelines

Per-packet load balancing allows the router to send data packets over successive equal-cost paths without regard to individual destination hosts or user sessions. Path utilization is good, but packets destined for a given destination host might take different paths and might arrive out of order.

Note Per-packet load balancing via CEF is not supported on Engine 2 Gigabit Switch Router (GSR) line cards (LCs).

Per-destination load balancing allows the router to use multiple, equal-cost paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple, equal-cost paths are available. Traffic for different source-destination host pairs tend to take different paths.

Note If you want to enable per-packet load sharing to a particular destination, then all interfaces that can forward traffic to the destination must be enabled for per-packet load sharing.

Examples

The following example enables per-packet load balancing:

```
interface E0
 ip load-sharing per-packet
```

The following example enables per-destination load balancing:

```
interface E0
 ip load-sharing per-destination
```

Related Commands

Command	Description
ip cef	Enables CEF on the RP card.

ip mroute-cache

To configure IP multicast fast switching or multicast distributed switching (MDS), use the **ip mroute-cache** command in interface configuration mode. To disable either of these features, use the **no** form of this command.

ip mroute-cache [**distributed**]

no ip mroute-cache [**distributed**]

Syntax Description

distributed	(Optional) Enables MDS on the interface. In the case of RSP, this keyword is optional; if it is omitted, fast switching occurs. On the GSR, this keyword is required because the GSR does only distributed switching.

Defaults

On the RSP, IP multicast fast switching is enabled; MDS is disabled.

On the GSR, MDS is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.

Usage Guidelines

On the RSP

If multicast fast switching is disabled on an incoming interface for a multicast routing table entry, the packet will be sent at process level for all interfaces in the outgoing interface list.

If multicast fast switching is disabled on an outgoing interface for a multicast routing table entry, the packet is process-level switched for that interface, but may be fast switched for other interfaces in the outgoing interface list.

When multicast fast switching is enabled (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching.

If MDS is not enabled on an incoming interface that is capable of MDS, incoming multicast packets will not be distributed switched; they will be fast switched at the Route Processor (RP) as before. Also, if the incoming interface is not capable of MDS, packets will get fast switched or process-switched at the RP as before.

If MDS is enabled on the incoming interface, but at least one of the outgoing interfaces cannot fast switch, packets will be process-switched. We recommend that you disable fast switching on any interface when MDS is enabled.

On the GSR

On the GSR, all interfaces should be configured for MDS because that is the only switching mode.

Examples

The following example enables IP multicast fast switching on the interface:

```
ip mroute-cache
```

The following example disables IP multicast fast switching on the interface:

```
no ip mroute-cache
```

The following example enables MDS on the interface:

```
ip mroute-cache distributed
```

The following example disables MDS and IP multicast fast switching on the interface:

```
no ip mroute-cache distributed
```

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing [**distributed**]

no ip multicast-routing

Syntax Description

distributed	(Optional) Enables MDS.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was introduced.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the **no** form of this command now disables IP multicast routing on the MMLS-RP and purges all multicast MLS cache entries on the MMLS-SE.

Usage Guidelines

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.

Examples

The following example enables IP multicast routing:

```
ip multicast-routing
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip route-cache

To control the use of switching methods for forwarding IP packets use the **ip route-cache** command in interface configuration mode. To disable any of these switching methods, use the **no** form of this command.

ip route-cache [**same-interface | flow | distributed | cef | policy**]

no ip route-cache [**same-interface | flow | distributed | cef | policy**]

Syntax Description

same-interface	Enables fast-switching packets to forward IP packets back out through the interface on which they arrived.
flow	Enables NetFlow accounting for packets that are received by the interface.
distributed	Enables distributed switching on the interface.
cef	Enables Cisco Express Forwarding (CEF) operation on an interface.
policy	Enables fast-switching for packets that are forwarded using Policy Based Routing (PBR).

Defaults

Fast Switching

The default behavior for Fast Switching varies by interface and media.

Distributed Switching

Distributed switching is disabled.

CEF and dCEF

When CEF or dCEF operation is enabled globally, all interfaces that support CEF or dCEF are enabled by default.

NetFlow

NetFlow accounting is disabled

Fast Switching for PBR (FSPBR)

FSPBR is disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **flow** keyword was added.
11.2GS	The **cef** and **distributed** keywords were added.
11.1CC	Support for multiple platforms was added for **cef** keyword.
12.0	The **policy** keyword was added.

Usage Guidelines

- ip route-cache
- ip route-cache same-interface
- ip route-cache flow
- ip route-cache distributed
- ip route-cache cef
- ip route-cache policy

ip route-cache

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis rather than on a per-packet basis. The **ip route-cache** command with no additional keywords enables fast switching.

Entering the **ip route-cache** command has no effect on a subinterface. Subinterfaces accept the **no** form of the command; however, this disables CEF or dCEF on the physical interface as well as all subinterfaces associated with the physical interface

ip route-cache same-interface

You can enable IP fast switching when the input and output interfaces are the same interface, using the **ip route-cache same-interface** command. This configuration normally is not recommended, although it is useful when you have partially meshed media, such as Frame Relay or you are running Web Cache Communication Protocol (WCCP) redirection. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection of packets to the optimal path.

ip route-cache flow

Enables (ingress) NetFlow accounting for traffic arriving on an interface.

ip route-cache distributed

The distributed option is supported on Cisco routers with line cards and Versatile Interface Processors (VIPs) that support both CEF and flow switching.

On Cisco routers with Route Switch Processor (RSP) and VIP controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. When VIP distributed switching is enabled, the input VIP interface tries to switch IP packets instead of forwarding them to the RSP for switching. Distributed switching helps decrease the demand on the RSP

ip route-cache cef

In some instances, you might want to disable CEF or dCEF on a particular interface because that interface is configured with a feature that CEF or dCEF does not support. Because all interfaces that support CEF or dCEF are enabled by default when you enable CEF operation globally, you must use the **no** form of the **ip route-cache cef** command in the interface configuration mode to turn CEF operation off a particular interface. To reenable CEF or dCEF operation, use the **ip route-cache cef** command.

Disabling CEF or dCEF on an interface disables CEF switching for packets forwarded to the interface, but has no effect on packets forwarded out of the interface.

Additionally when you disable CEF or dCEF, Cisco IOS software switches packets using the next-fastest switching path. In the case of dCEF, the next-fastest switching path is CEF on the RSP.

Note On the Cisco 12000 Series Internet Router, you must not disable dCEF on an interface

ip route-cache policy

1. If Cisco Express Forwarding (CEF) is already enabled, this command is not needed because PBR packets are CEF switched by default.
2. Before you can enable fast-switched PBR, PBR itself must be configured.
3. FSPBR supports all of PBR's **match** commands and most of PBR's **set** commands, with the following restrictions:
   - The **set ip default next-hop** and **set default interface** commands are not supported.
   - The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.

Examples

- Configuring Fast Switching and Disabling CEF Switching
- Configuring Fast Switching for Traffic That is Received and Transmitted Over the Same Interface
- Enabling NetFlow Accounting
- Configuring Distributed Switching
- Configuring Fast Switching for PBR

Configuring Fast Switching and Disabling CEF Switching

The following example shows how to enable fast switching and disable CEF switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache
```

The following example shows that fast switching is enabled:

```
Router# show ip interface fastEthernet 0/0/0
FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
```

The following example shows that CEF switching is disabled:

```
Router# show cef interface fastEthernet 0/0/0
FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP CEF switching disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500
```

The following example shows the configuration information for interface fastethernet 0/0/0

```
Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 no ip route-cache cef
 no ip route-cache distributed
!
```

Configuring Fast Switching for Traffic That is Received and Transmitted Over the Same Interface

The following example shows how to enable fast switching and disable CEF switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache same-interface
```

The following example shows that fast switching on the same interface is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0
FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
```

```
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
```

The following example shows the configuration information for interface fastethernet 0/0/0

```
Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 ip route-cache same-interface
 no ip route-cache cef
 no ip route-cache distributed
!
```

Enabling NetFlow Accounting

The following example shows how to enable NetFlow switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache flow
```

The following example shows that NetFlow accounting is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0
FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is enabled
```

```
  IP Distributed switching is disabled
  IP Flow switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Flow
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
```

Configuring Distributed Switching

The following example shows how to enable distributed switching:

```
Router(config)# ip cef distributed
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache distributed
```

The following example shows that distributed CEF switching is for interface fastethernet 0/0/0:

```
Router# show cef interface fastEthernet 0/0/0
FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500
```

Configuring Fast Switching for PBR

The following example shows how to configure a simple policy based routing scheme and to enable FSPBR:

```
Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# route-map my_pbr_tag permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set ip next-hop 10.1.1.195
Router(config-route-map)# exit
Router(config)# interface fastethernet 0/0/0
```

```
Router(config-if)# ip route-cache policy
Router(config-if)# ip policy route-map my_pbr_tag
```

The following example shows that FSPBR is enabled for interface fastethernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0
FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Distributed switching is enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Distributed, Policy, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is enabled, using route map my_pbr_tag
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled
```

Related Commands

Command	Description
ip cef	Enables CEF on the RP card.
ip cef distributed	Enables distributed CEF (dCEF) operation.
show ip interface	Displays the usability status of interfaces configured for IP.
show cef interface	Displays detailed Cisco Express Forwarding (CEF) information for interfaces.

ip route-cache policy

To enable fast-switch Policy Based Routing (PBR), use the **ip route-cache policy** command in interface configuration mode. To disable fast-switched PBR, use the **no** form of this command.

[no] ip route-cache policy

Syntax Description

This command has no arguments or keywords.

Defaults

Not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

1. If Cisco Express Forwarding (CEF) is already enabled, the present command isn't needed, because PBR packets are CEF switched by default.
2. Before you can enable fast-switch PBR, PBR itself must be configured.
3. FSPBR supports all of PBR's **match** commands and most of PBR's **set** commands, with the following restrictions:
   - The **set ip default next-hop** and **set default interface** commands are not supported.
   - The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.

Examples

The following example enables fast-switch Policy Based Routing on an Ethernet interface:

```
Router# config t
   Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int e 1/3
Router(config-if)# ip route-cache policy
Router(config-if)# end
```

Related Commands

Command	Description
show ip cache policy	Displays cache entries in the policy route-cache.

ip route vrf

To establish static routes for a 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 VPN routing/forwarding instance (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: ATM, Ethernet, loopback, POS (packet over SONET), or null.
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.

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, 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 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.

Examples

The following command reroutes packets addressed to network 137.23.0.0 in VRF vpn3 to router 131.108.6.6:

```
ip route vrf vpn3 137.23.0.0 255.255.0.0 131.108.6.6
```

Related Commands

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

ip vrf forwarding

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

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

The default for an interface is the global routing table.

Command Modes

Global configuration

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

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.

Examples

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

```
interface atm0/0
ip vrf forwarding vpn1
```

Related Commands

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

ip vrf

To configure a VPN routing and forwarding (VRF) routing table, use the **ip vrf** command in global configuration mode or router configuration mode. To remove a VRF routing table, 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.

Defaults

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

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF routing table and a Cisco Express Forwarding (CEF) table, both named *vrf-name*. Associated with these tables is the default route distinguisher value *route-distinguisher*.

Examples

The following example imports a route map to a VRF:

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

Related Commands

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

keepalive-lifetime

To specify the duration that a keepalive message from an MPS is considered valid by the MPC, use the **keepalive-lifetime** command in global configuration mode.

keepalive-lifetime *time*

Syntax Description

time	Time (in seconds) for the MPS-p2 variable of the MPS. The default value is 35 seconds.

Defaults

The default is 35 seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The keepalive lifetime (MPS-p2) must be greater than or equal to three times the value of the keepalive time (MPS-p1). MPS-p1 specifies the frequency with which a keepalive message is sent from the MPS to the MPC.

Examples

The following example specifies a keepalive lifetime of 60 seconds:

```
keepalive-lifetime 60
```

Related Commands

Command	Description
keepalive-time	Specifies the keepalive time value for the MPS-p1 variable of an MPS.

keepalive-time

To specify the keepalive time value for the MPS-p1variable of an MPS, use the **keepalive-time** command in MPS configuration mode. To revert to the default value, use the **no** form of this command.

keepalive-time *time*

no keepalive-time *time*

Syntax Description

time	Specifies the keepalive time value (in seconds).

Defaults

The default keepalive time is 10 seconds.

Command Modes

MPS configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Examples

The following example sets the keepalive time to 25 seconds:

```
keepalive-time 25
```

lane auto-config-atm-address

To specify that the configuration server ATM address is computed by the Cisco automatic method, use the **lane auto-config-atm-address** command in interface configuration mode. To remove the previously assigned ATM address, use the **no** form of this command.

lane [**config**] **auto-config-atm-address**

no lane [**config**] **auto-config-atm-address**

Syntax Description

config	(Optional) When the **config** keyword is used, this command applies only to the LAN Emulation Configuration Server (LECS). This keyword indicates that the LECS should use the auto computed LECS address.

Defaults

No specific ATM address is set.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

When the **config** keyword is not present, this command causes the LANE server and LANE client on the subinterface to use the automatically assigned ATM address for the configuration server.

When the **config** keyword is present, this command assigns the automatically generated ATM address to the configuration server (LECS) configured on the interface. Multiple commands that assign ATM addresses to the LANE configuration server can be issued on the same interface to assign different ATM addresses to the configuration server. Commands that assign ATM addresses to the LANE configuration server include **lane auto-config-atm-address**, **lane config-atm-address**, and **lane fixed-config-atm-address**.

For a discussion of Cisco's method of automatically assigning ATM addresses, refer to the "Configuring LAN Emulation" chapter in the *Cisco IOS Switching Services Configuration Guide.*

Examples

The following example associates the LANE configuration server with the database named network1 and specifies that the configuration server's ATM address will be assigned by the Cisco automatic method:

```
lane database network1
 name eng server-atm-address 39.020304050607080910111213.0800.AA00.1001.02
 name mkt server-atm-address 39.020304050607080910111213.0800.AA00.4001.01
interface atm 1/0
 lane config database network1
 lane config auto-config-atm-address
```

The following example causes the LANE server and LANE client on the subinterface to use the automatically assigned ATM address to communicate with the configuration server:

```
interface atm 2/0.1
 ip address 172.16.0.4 255.255.255.0
 lane client ethernet
 lane server-bus ethernet eng
 lane auto-config-atm-address
```

Related Commands

Command	Description
lane config-atm-address	Specifies the ATM address of the configuration server explicitly.
lane database	Creates a named configuration database that can be associated with a configuration server.
lane fixed-config-atm-address	Specifies that the fixed configuration server ATM address assigned by the ATM Forum will be used.

lane bus-atm-address

To specify an ATM address—and thus override the automatic ATM address assignment—for the broadcast and unknown server on the specified subinterface, use the **lane bus-atm-address** command in interface configuration mode. To remove the ATM address previously specified for the broadcast and unknown server on the specified subinterface and thus revert to the automatic address assignment, use the **no** form of this command.

lane bus-atm-address *atm-address-template*

no lane bus-atm-address [*atm-address-template*]

Syntax Description

atm-address-template	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the end-system identifier (ESI) bytes, or the selector byte of the automatically assigned ATM address.

Defaults

For the broadcast and unknown server, the default is automatic ATM address assignment.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

When applied to a broadcast and unknown server, this command overrides automatic ATM address assignment for the broadcast and unknown server. When applied to a LANE client, this command gives the client the ATM address of the broadcast and unknown server. The client will use this address rather than sending LE ARP requests for the broadcast address.

When applied to a selected interface, but with a different ATM address from what was used previously, this command replaces the broadcast and unknown server's ATM address.

ATM Addresses

A LANE ATM address has the same syntax as an NSAP (but it is not a network-level address). It consists of the following:

- A 13-byte prefix that includes the following fields defined by the ATM Forum:
  - AFI (Authority and Format Identifier) field (1 byte)
  - DCC (Data Country Code) or ICD (International Code Designator) field (2 bytes)
  - DFI field (Domain Specific Part Format Identifier) (1 byte)
  - Administrative Authority field (3 bytes)
  - Reserved field (2 bytes)

  - Routing Domain field (2 bytes)
  - Area field (2 bytes)
- A 6-byte ESI
- A 1-byte selector field

Address Templates

LANE ATM address templates can use two types of wildcards: an asterisk (*) to match any single character (nibble), and an ellipsis (...) to match any number of leading, middle, or trailing characters. The values of the characters replaced by wildcards come from the automatically assigned ATM address.

The values of the digits that are replaced by wildcards come from the automatic ATM assignment method.

In LANE, a *prefix template* explicitly matches the prefix but uses wildcards for the ESI and selector fields. An *ESI template* explicitly matches the ESI field but uses wildcards for the prefix and selector.

The Cisco implementation of LANE, the prefix corresponds to the switch, the ESI corresponds to the ATM interface, and the selector field corresponds to the specific subinterface of the interface.

Examples

The following example uses an ESI template to specify the part of the ATM address corresponding to the interface; the remaining values in the ATM address come from automatic assignment:

```
lane bus-atm-address ...0800.200C.1001.**
```

The following example uses a prefix template to specify the part of the ATM address corresponding to the switch; the remaining values in the ATM address come from automatic assignment:

```
lane bus-atm-address 45.000014155551212f.00.00...
```

Related Commands

Command	Description
lane server-bus	Enables a LANE server and a broadcast and unknown server on the specified subinterface with the ELAN ID.

lane client

To activate a LANE client on the specified subinterface, use the **lane client** command in interface configuration mode. To remove a previously activated LANE client on the subinterface, use the **no** form of this command.

lane client {**ethernet** | **tokenring**} [*elan-name*]

no lane client [{**ethernet** | **tokenring**} [*elan-name*]]

Syntax Description

ethernet	Identifies the emulated LAN (ELAN) attached to this subinterface as an Ethernet ELAN.
tokenring	Identifies the ELAN attached to this subinterface as a Token Ring ELAN.
elan-name	(Optional) Name of the ELAN. This argument is optional because the client obtains its ELAN name from the configuration server. The maximum length of the name is 32 characters.

Defaults

No LANE clients are enabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If a **lane client** command has already been used on the subinterface for a different ELAN, then the client initiates termination procedures for that emulated LAN and joins the new ELAN.

If you do not provide an *elan-name* value, the client contacts the server to find which emulated LAN to join. If you do provide an ELAN name, the client consults the configuration server to ensure that no conflicting bindings exist.

Examples

The following example enables a Token Ring LANE client on an interface:

```
lane client tokenring
```

Related Commands

Command	Description
lane client-atm-address	Specifies an ATM address—and thus overrides the automatic ATM address assignment—for the LANE client on the specified subinterface.

lane client-atm-address

To specify an ATM address—and thus override the automatic ATM address assignment—for the LANE client on the specified subinterface, use the **lane client-atm-address** command in interface configuration mode. To remove the ATM address previously specified for the LANE client on the specified subinterface and thus revert to the automatic address assignment, use the **no** form of this command.

lane client-atm-address *atm-address-template*

no lane client-atm-address [*atm-address-template*]

Syntax Description

atm-address-template	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the ESI bytes, or the selector byte of the automatically assigned ATM address.

Defaults

Automatic ATM address assignment

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use of this command on a selected subinterface, but with a different ATM address from what was used previously, replaces ATM address of the LANE client.

ATM Addresses

A LANE ATM address has the same syntax as an NSAP (but it is not a network-level address). It consists of the following:

- A 13-byte prefix that includes the following fields defined by the ATM Forum:
  - AFI (Authority and Format Identifier) field (1 byte)
  - DCC (Data Country Code) or ICD (International Code Designator) field (2 bytes)
  - DFI field (Domain Specific Part Format Identifier) (1 byte)
  - Administrative Authority field (3 bytes)
  - Reserved field (2 bytes)
  - Routing Domain field (2 bytes)
  - Area field (2 bytes)
- A 6-byte ESI
- A 1-byte selector field

Address Templates

LANE ATM address templates can use two types of wildcards: an asterisk (*) to match any single character (nibble), and an ellipsis (...) to match any number of leading, middle, or trailing characters. The values of the characters replaced by wildcards come from the automatically assigned ATM address.

In LANE, a *prefix template* explicitly matches the ATM address prefix but uses wildcards for the ESI and selector fields. An *ESI template* explicitly matches the ESI field but uses wildcards for the prefix and selector.

The Cisco implementation of LANE, the prefix corresponds to the switch, the ESI corresponds to the ATM interface, and the selector field corresponds to the specific subinterface of the interface.

For a discussion of Cisco's method of automatically assigning ATM addresses, refer to the "Configuring LAN Emulation" chapter in the *Cisco IOS Switching Services Configuration Guide*.

Examples

The following example uses an ESI template to specify the part of the ATM address corresponding to the interface; the remaining parts of the ATM address come from automatic assignment:

```
lane client-atm-address...0800.200C.1001.**
```

The following example uses a prefix template to specify the part of the ATM address corresponding to the switch; the remaining parts of the ATM address come from automatic assignment:

```
lane client-atm-address 47.000014155551212f.00.00...
```

Related Commands

Command	Description
lane client	Activates a LANE client on the specified subinterface.

lane client flush

To enable the flush mechanism of a LAN Emulation Client (LEC), use the **lane client flush** global configuration command. To disable the flush mechanism of a LEC, use the **no** form of this command.

lane client flush

no lane client flush

Syntax Description

This command contains no arguments or keywords.

Defaults

All the LECs perform the LANE LE_FLUSH process by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

In Cisco IOS Release 12.1(3)T and later releases, the **lane client flush** command will be hidden and will not be visible in the configuration.

Configuring the **no lane client flush** command on a Cisco networking device is recommended to prevent the initial packet drops during the establishment of LANE data direct virtual connection (VCC).

Use the **no lane client flush** command to keep LANE clients from sending LE_FLUSH messages to the remote LANE client. This will also allow the LANE clients to process the LE_FLUSH messages *from* the remote LANE clients.

Note Configuring the **no lane client flush** command on a Cisco networking device does not guarantee the orderly delivery of incoming packets. There is a chance of receiving out-of-order packets at the destination during the establishment of a LANE data direct VCC.

Examples

The following example disables the flush mechanism of a LEC:

```
no lane client flush
```

Related Commands

Command	Description
lane client	Activates a LANE client on the specified subinterface.
lane client-atm-address	Specifies an ATM address—and thus overrides the automatic ATM address assignment—for the LANE client on the specified subinterface.

lane client mpoa client name

To bind a LEC to the named MPC, use the **lane client mpoa client name** command in interface configuration mode. To unbind the named MPC from a LEC, use the **no** form of this command.

lane client mpoa client name *mpc-name*

no lane client mpoa client name *mpc-name*

Syntax Description

mpc-name	Name of the specific MPC.

Defaults

No LEC is bound to a named MPC.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

When you enter this command, the named MPC is bound to a LEC. The named MPC must exist before this command is accepted. If you enter this command before a LEC is configured (not necessarily running), a warning message is issued.

Examples

The following example binds a LEC on a subinterface to the MPC:

```
lane client mpoa client name ip_mpc
```

lane client mpoa server name

To bind a LEC with the named MPS, use the **lane client mpoa server name** command in interface configuration mode. To unbind the server, use the **no** form of this command.

lane client mpoa server name *mps-name*

no lane client mpoa server name *mps-name*

Syntax Description

mps-name	Name of the specific MPOA server.

Defaults

No LEC is bound to a named MPS.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

This command binds a LEC to the named MPS. The specified MPS must exist before this command is accepted. If this command is entered when a LEC is not already configured (not necessarily running), a warning message will be issued.

Examples

The following example binds a LANE client with the MPS named MYMPS:

```
lane client mpoa server name MYMPS
```

lane config-atm-address

To specify a configuration server's ATM address explicitly, use the **lane config-atm-address** command in interface configuration mode. To remove an assigned ATM address, use the **no** form of this command.

lane [**config**] **config-atm-address** *atm-address-template*

no lane [**config**] **config-atm-address** *atm-address-template*

Syntax Description

config	(Optional) When the **config** keyword is used, this command applies only to the LANE Configuration Server (LECS). This keyword indicates that the LECS should use the 20-byte address that you explicitly entered.
atm-address-template	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the ESI bytes, or the selector byte of the automatically assigned ATM address.

Defaults

No specific ATM address or method is set.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If the **config** keyword is not present, this command causes the LANE server and LANE client on the subinterface to use the specified ATM address for the configuration server.

When the **config** keyword is present, this command adds an ATM address to the configuration server configured on the interface. A LECS can listen on multiple ATM addresses. Multiple commands that assign ATM addresses to the LECS can be issued on the same interface to assign different ATM addresses to the LECS.

ATM Addresses

A LANE ATM address has the same syntax as an NSAP (but it is not a network-level address). It consists of the following:

- A 13-byte prefix that includes the following fields defined by the ATM Forum:
  - AFI (Authority and Format Identifier) field (1 byte)
  - DCC (Data Country Code) or ICD (International Code Designator) field (2 bytes)
  - DFI field (Domain Specific Part Format Identifier) (1 byte)
  - Administrative Authority field (3 bytes)
  - Reserved field (2 bytes)

  - Routing Domain field (2 bytes)
  - Area field (2 bytes)
- A 6-byte ESI
- A 1-byte selector field

Address Templates

LANE ATM address templates can use two types of wildcards: an asterisk (*) to match any single character (nibble), and an ellipsis (...) to match any number of leading, middle, or trailing characters. The values of the characters replaced by wildcards come from the automatically assigned ATM address.

In LANE, a *prefix template* explicitly matches the ATM address prefix but uses wildcards for the ESI and selector fields. An *ESI template* explicitly matches the ESI field but uses wildcards for the prefix and selector.

In our implementation of LANE, the prefix corresponds to the switch prefix, the ESI corresponds to a function of the ATM interface's MAC address, and the selector field corresponds to the specific subinterface of the interface.

For a discussion of the Cisco method of automatically assigning ATM addresses, refer to the "Configuring LAN Emulation" chapter in the *Cisco IOS Switching Services Configuration Guide*.

Examples

The following example associates the LANE configuration server with the database named network1 and explicitly specifies the configuration server's ATM address:

```
lane database network1
 name eng server-atm-address 39.020304050607080910111213.0800.AA00.1001.02
 name mkt server-atm-address 39.020304050607080910111213.0800.AA00.4001.01
interface atm 1/0
 lane config database network1
 lane config config-atm-address 39.020304050607080910111213.0800.AA00.3000.00
```

The following example causes the LANE server and LANE client on the subinterface to use the explicitly specified ATM address to communicate with the configuration server:

```
interface atm 2/0.1
 ip address 172.16.0.4 255.255.255.0
 lane client ethernet
 lane server-bus ethernet eng
 lane config-atm-address 39.020304050607080910111213.0800.AA00.3000.00
```

Related Commands

Command	Description
lane auto-config-atm-address	Specifies that the configuration server ATM address is computed by the Cisco automatic method.
lane config database	Associates a named configuration table (database) with the configuration server on the selected ATM interface.
lane database	Creates a named configuration database that can be associated with a configuration server.
lane fixed-config-atm-address	Specifies that the fixed configuration server ATM address assigned by the ATM Forum will be used.

lane config database

To associate a named configuration table (database) with the configuration server on the selected ATM interface, use the **lane config database** command in interface configuration mode. To remove the association between a named database and the configuration server on the specified interface, use the **no** form of this command.

lane config database *database-name*

no lane config database

Syntax Description

database-name	Name of the LANE database.

Defaults

No configuration server is defined, and no database name is provided.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command is valid only on a major interface, not a subinterface, because only one LANE Configuration Server (LECS) can exist per interface.

The named database must exist before the **lane config database** command is used. Refer to the **lane database** command for more information.

Multiple **lane config database** commands cannot be used multiple times on the same interface. You must delete an existing association by using the **no** form of this command before you can create a new association on the specified interface.

Activating a LANE configuration server requires the **lane config database** command and one of the following commands: **lane fixed-config-atm-address**, **lane auto-config-atm-address**, or **lane config-atm-address**.

Examples

The following example associates the LECS with the database named network1 and specifies that the configuration server's ATM address will be assigned by the Cisco automatic method:

```
lane database network1
 name eng server-atm-address 39.020304050607080910111213.0800.AA00.1001.02
 name mkt server-atm-address 39.020304050607080910111213.0800.AA00.4001.01
interface atm 1/0
 lane config database network1
 lane config auto-config-atm-address
```

Related Commands

Command	Description
lane auto-config-atm-address	Specifies that the configuration server ATM address is computed by the Cisco automatic method.
lane config-atm-address	Specifies the ATM address of the configuration server explicitly.
lane database	Creates a named configuration database that can be associated with a configuration server.
lane fixed-config-atm-address	Specifies that the fixed configuration server ATM address assigned by the ATM Forum will be used.

lane database

To create a named configuration database that can be associated with a configuration server, use the **lane database** command in global configuration mode. To delete the database, use the **no** form of this command.

lane database *database-name*

no lane database *database-name*

Syntax Description

database-name	Database name (32 characters maximum).

Defaults

No name is provided.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use of the **lane database** command places you in database configuration mode, in which you can use the **client-atm-address name, default name, mac-address name, name restricted, name unrestricted, name new-name,** and **name server-atm-address** commands to create entries in the specified database. When you are finished creating entries, type **^Z** or **exit** to return to global configuration mode.

Examples

The following example creates the database named network1 and associates it with the configuration server on interface ATM 1/0:

```
lane database network1
 name eng server-atm-address 39.020304050607080910111213.0800.AA00.1001.02
 name mkt server-atm-address 39.020304050607080910111213.0800.AA00.4001.01
 default-name eng
interface atm 1/0
 lane config database network1
 lane config auto-config-atm-address
```

Related Commands

Command	Description
client-atm-address name	Adds a LANE client address entry to the configuration database of the configuration server.
default-name	Provides an ELAN name in the database of the configuration server for those client MAC addresses and client ATM addresses that do not have explicit ELAN name bindings.

Command	Description
lane config database	Associates a named configuration table (database) with the configuration server on the selected ATM interface.
mac-address	Sets the MAC-layer address of the Cisco Token Ring.
name	Assigns a name to the internal adapter.
name server-atm-address	Specifies or replaces the ATM address of the LANE server for the ELAN in the configuration database of the configuration server.

lane fixed-config-atm-address

To specify that the fixed configuration server ATM address assigned by the ATM Forum will be used, use the **lane fixed-config-atm-address** command in interface configuration mode. To specify that the fixed ATM address will not be used, use the **no** form of this command.

lane [**config**] **fixed-config-atm-address**

no lane [**config**] **fixed-config-atm-address**

Syntax Description

config	(Optional) When the **config** keyword is used, this command applies only to the LANE Configuration Server (LECS). This keyword indicates that LECS should use the well-known, ATM Forum LEC address.

Defaults

No specific ATM address or method is set.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

When the **config** keyword is not present, this command causes the LANE server and LANE client on the subinterface to use that ATM address, rather than the ATM address provided by the ILMI, to locate the configuration server.

When the **config** keyword is present, and the LECS is already up and running, be aware of the following scenarios:

- If you configure the LECS with only the well-known address, the LECS will not participate in the SSRP, will act as a standalone master, and will listen only on the well-known LECS address. This scenario is ideal if you want a standalone LECS that does not participate in SSRP, and you would like to listen to only the well-known address.
- If only the well-known address is already assigned, and you assign at least one other address to the LECS (additional addresses are assigned using the **lane auto-config-atm-address** command or the **lane config-atm-address** command), the LECS will participate in the SSRP and act as the master or slave based on the normal SSRP rules. This scenario is ideal if you would like the LECS to participate in SSRP, and you would like to make the master LECS listen on the well-known address.
- If the LECS is participating in SSRP, has more than one address (one of which is the well-known address), and all the addresses but the well-known address are removed, the LECS will declare itself the master and stop participating in SSRP completely.
- If the LECS is operating as an SSRP slave, and it has the well-known address configured, it will not listen on the well-known address unless it becomes the master.
- If you want the LECS to assume the well-known address only when it becomes the master, configure the LECS with the well-known address and at least one other address.

When you use this command with the **config** keyword, and the LECS is a master, the master will listen on the fixed address. If you use this command when an LECS is not a master, the LECS will listen on this address when it becomes a master. If you do not use this command, the LECS will not listen on the fixed address.

Multiple commands that assign ATM addresses to the LECS can be issued on the same interface in order to assign different ATM addresses to the LECS. Commands that assign ATM addresses to the LECS include **lane auto-config-atm-address, lane config-atm-address**, and **lane fixed-config-atm-address**. The **lane config database** command and at least one command that assigns an ATM address to the LECS are required to activate a LECS.

Examples

The following example associates the LECS with the database named network1 and specifies that the configuration server's ATM address is the fixed address:

```
lane database network1
 name eng server-atm-address 39.020304050607080910111213.0800.AA00.1001.02
 name mkt server-atm-address 39.020304050607080910111213.0800.AA00.4001.01
interface atm 1/0
 lane config database network1
 lane config fixed-config-atm-address
```

The following example causes the LANE server and LANE client on the subinterface to use the fixed ATM address to communicate with the configuration server:

```
interface atm 2/0.1
 ip address 172.16.0.4 255.255.255.0
 lane client ethernet
 lane server-bus ethernet eng
 lane fixed-config-atm-address
```

Related Commands

Command	Description
lane auto-config-atm-address	Specifies that the configuration server ATM address is computed by the Cisco automatic method.
lane config-atm-address	Specifies the ATM address of the configuration server explicitly.
lane config database	Associates a named configuration table (database) with the configuration server on the selected ATM interface.

lane fssrp

To enable the special LANE features such that LANE components (such as the LANE Configuration Server, the LANE client, the LANE server, and the BUS) become aware of FSSRP, use the **lane fssrp** command in interface configuration mode. To disable the LANE FSSRP configuration, use the **no** form of this command.

lane fssrp

no lane fssrp

Syntax Description

This command contains no keywords or arguments.

Defaults

FSSRP is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(4c)W5(10a)	This command was introduced.

Usage Guidelines

You must execute this command on all ATM interfaces to enable FSSRP capability for all LANE components on that interface and hence all its subinterfaces.

Examples

The following example enables FSSRP on an ATM interface:

```
lane fssrp
```

Related Commands

Command	Description
lane client	Activates a LANE client on the specified subinterface.
lane server	Activates a LANE server on the specified subinterface.
show lane client	Generates additional FSSRP information about a LANE client.
show lane config	Displays global LANE information for the configuration server configured on an interface.

lane global-lecs-address

To specify a list of LECS addresses to use when the addresses cannot be obtained from the ILMI, use the **lane global-lecs-address** command in interface configuration mode. To remove a LECS address from the list, use the **no** form of this command.

lane global-lecs-address *address*

no lane global-lecs-address *address*

Syntax Description

address	Address of the LECS. You cannot use the well-known LECS address.

Defaults

No addresses are configured. The router obtains LECS addresses from the ILMI.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command when your ATM switches do not support the ILMI list of LECS addresses and you want to configure Simple Server Redundancy. This command will simulate the list of LECS addresses, as if they had been obtained from the ILMI. Use this command with a different address for each LECS. The order they are used determines their priority. You should enter the addresses in the same order as you would on the ATM switch.

Note You must configure the same list of addresses on each interface that contains a LANE entity.

If your switches do support ILMI, this command forces the router to use the addresses specified and will not use the ILMI to obtain the LECS addresses.

Because the well-known LECS address is always used as a last resort LECS address, you cannot use the address in this command.

lane le-arp

To add a static entry to the LE ARP table of the LANE client configured on the specified subinterface, use the **lane le-arp** command in interface configuration mode. To remove a static entry from the LE ARP table of the LANE client on the specified subinterface, use the **no** form of this command.

lane le-arp {*mac-address* | **route-desc segment** *segment-number* **bridge** *bridge-number*} *atm-address*

no lane le-arp {*mac-address* | **route-desc segment** *segment-number* **bridge** *bridge-number*} *atm-address*

Syntax Description

mac-address	MAC address to bind to the specified ATM address.
route-desc segment *segment-number*	LANE segment number. The segment number ranges from 1 to 4095.
bridge *bridge-number*	Bridge number that is contained in the route descriptor. The bridge number ranges from 1 to 15.
atm-address	ATM address.

Defaults

No static address bindings are provided.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command adds or removes a static entry binding a MAC address or segment number and bridge number to an ATM address. It does not add or remove dynamic entries. Removing the static entry for a specified ATM address from a LE ARP table does not release data direct VCCs established to that ATM address. However, clearing a static entry clears any fast-cache entries that were created from the MAC address-to-ATM address binding.

Static LE ARP entries are neither aged nor removed automatically.

To remove dynamic entries from the LE ARP table of the LANE client on the specified subinterface, use the **clear lane le-arp** command.

Examples

The following example adds a static entry to the LE ARP table:

```
lane le-arp 0800.aa00.0101 47.000014155551212f.00.00.0800.200C.1001.01
```

The following example adds a static entry to the LE ARP table binding segment number 1, bridge number 1 to the ATM address:

```
lane le-arp route-desc segment 1 bridge 1 39.0203040506070809101112l3.00000CA05B41.01
```

Related Commands

Command	Description
clear lane le-arp	Forces a LANE server to drop a client and allow the LANE configuration server to assign the client to another ELAN.

lane server-atm-address

To specify an ATM address—and thus override the automatic ATM address assignment—for the LANE server on the specified subinterface, use the **lane server-atm-address** command in interface configuration mode. To remove the ATM address previously specified for the LANE server on the specified subinterface and thus revert to the automatic address assignment, use the **no** form of this command.

lane server-atm-address *atm-address-template*

no lane server-atm-address [*atm-address-template*]

Syntax Description

atm-address-template	ATM address or a template in which wildcard characters are replaced by any nibble or group of nibbles of the prefix bytes, the ESI bytes, or the selector byte of the automatically assigned ATM address.

Defaults

For the LANE server, the default is automatic address assignment; the LANE client finds the LANE server by consulting the configuration server.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command also instructs the LANE client configured on this subinterface to reach the LANE server by using the specified ATM address instead of the ATM address provided by the configuration server.

When used on a selected subinterface, but with a different ATM address than was used previously, this command replaces the ATM address of the LANE server.

ATM Addresses

A LANE ATM address has the same syntax as an NSAP (but it is not a network-level address). It consists of the following:

- A 13-byte prefix that includes the following fields defined by the ATM Forum:
  - AFI (Authority and Format Identifier) field (1 byte)
  - DCC (Data Country Code) or ICD (International Code Designator) field (2 bytes)
  - DFI field (Domain Specific Part Format Identifier) (1 byte)
  - Administrative Authority field (3 bytes)
  - Reserved field (2 bytes)
  - Routing Domain field (2 bytes)
  - Area field (2 bytes)

- A 6-byte ESI
- A 1-byte selector field

Address Templates

LANE ATM address templates can use two types of wildcards: an asterisk (*) to match any single character (nibble), and an ellipsis (...) to match any number of leading, middle, or trailing characters. The values of the characters replaced by wildcards come from the automatically assigned ATM address.

In LANE, a *prefix template* explicitly matches the prefix, but uses wildcards for the ESI and selector fields. An *ESI template* explicitly matches the ESI field, but uses wildcards for the prefix and selector.

In the Cisco implementation of LANE, the prefix corresponds to the switch, the ESI corresponds to the ATM interface, and the selector field corresponds to the specific subinterface of the interface.

For a discussion of the Cisco method of automatically assigning ATM addresses, refer to the "Configuring LAN Emulation" chapter of the *Cisco IOS Switching Services Configuration Guide*.

Examples

The following example uses an ESI template to specify the part of the ATM address corresponding to the interface; the remaining parts of the ATM address come from automatic assignment:

```
lane server-atm-address ...0800.200C.1001.**
```

The following example uses a prefix template to specify the part of the ATM address corresponding to the switch; the remaining part of the ATM address come from automatic assignment:

```
lane server-atm-address 45.000014155551212f.00.00...
```

Related Commands

Command	Description
lane server-bus	Enables a LANE server and a BUS on the specified subinterface with the ELAN ID.

lane server-bus

To enable a LANE server and a broadcast and unknown server (BUS) on the specified subinterface with the ELAN ID, use the **lane server-bus** command in interface configuration mode. To disable a LANE server and BUS on the specified subinterface, use the **no** form of this command.

lane server-bus {**ethernet** | **tokenring**} *elan-name* [**elan-id** *id*]

no lane server-bus {**ethernet** | **tokenring**} *elan-name* [**elan-id** *id*]

Syntax Description

ethernet	Identifies the emulated LAN (ELAN) attached to this subinterface as an Ethernet ELAN.
tokenring	Identifies the ELAN attached to this subinterface as a Token Ring ELAN.
elan-name	Name of the ELAN. The maximum length of the name is 32 characters.
elan-id	(Optional) Identifies the ELAN.
id	(Optional) Specifies the ELAN ID of the LEC.

Defaults

No LAN type or ELAN name is provided.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0	This command was modified to support the **elan-id** keyword.

Usage Guidelines

The LANE server and the BUS are located on the same router.

If a **lane server-bus** command has already been used on the subinterface for a different ELAN, the server initiates termination procedures with all clients and comes up as the server for the new ELAN.

To participate in MPOA, a LEC must have an ELAN ID. This command enables the LEC to get the ELAN ID from the LES when the LEC bypasses the LECS phase.

Caution If an ELAN ID is supplied, make sure that it corresponds to the same ELAN ID value specified in the LECS for the same ELAN.

The LEC can also obtain the ELAN ID from the LECS by using the **name elan-id** command.

Examples

The following example enables a LANE server and BUS for a Token Ring ELAN named MYELAN:

```
lane server-bus tokenring myelan
```

Related Commands

Command	Description
lane server-atm-address	Specifies an ATM address and thus overrides the automatic ATM address assignment for the LANE server on a specified subinterface.
name elan-id	Configures the ELAN ID of an ELAN in the LECS database to participate in MPOA.

list

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

list [*starting-index-number*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

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

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

Explicit Path name Joe:
    1:next-address 10.0.0.1
    2:next-address 10.0.0.2

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

Explicit Path name Joe:
    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.

mask destination

To specify the destination mask, use the **mask destination** destination-prefix aggregation cache configuration command. To disable the destination mask, use the **no** form of this command.

mask destination minimum *value*

no mask destination minimum *value*

Syntax Description

minimum	Configures the minimum value for the mask.
value	Specifies the value for the mask. Range is from 1 to 32.

Defaults

0

Command Modes

Destination-prefix aggregation cache configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is only available with router-based aggregation. Minimum masking capability is not available if router-based aggregation is not enabled.

Examples

The following example shows how to configure the destination-prefix aggregation cache with a minimum mask value:

```
ip flow-aggregation cache destination-prefix
mask destination minimum 32
```

Related Commands

Command	Description
ip flow-aggregation cache	Enables aggregation cache configuration mode.
mask source	Specifies the source mask.
show ip cache flow aggregation	Displays the aggregation cache configuration.

mask source

To specify the source mask, use the **mask source** source-prefix aggregation cache configuration command. To disable the source mask, use the **no** form of this command.

mask source minimum *value*

no mask source minimum *value*

Syntax Description

minimum	Configures the minimum value for the mask.
value	Specifies the value for the mask. Range is from 1 to 32.

Defaults

0

Command Modes

Source-prefix aggregation cache

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is only available with router-based aggregation. Minimum masking capability is not available if router-based aggregation is not enabled.

Examples

The following example shows how to configure the source-prefix aggregation cache with a minimum mask value:

```
ip flow-aggregation cache source-prefix
mask source minimum 30
```

Related Commands

Command	Description
ip flow-aggregation cache	Enables aggregation cache configuration mode.
mask destination	Specifies the destination mask.
show ip cache flow aggregation	Displays the aggregation cache configuration.

maximum routes

To limit the maximum number of routes in a VRF to prevent a PE router from importing too many routes, use the **maximum routes** command in VRF configuration submode. To remove the limit on the maximum number of routes allowed, use the **no** form of this command.

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

no maximum routes

Syntax Description

limit	Specifies the maximum number of routes allowed in a VRF. You may select from 1 to 4,294,967,295 routes to be allowed in a VRF.
warn threshold	Rejects routes when the threshold limit is reached. The threshold limit is a percentage of the limit specified, from 1 to 100.
warn-only	Issues a syslog error message when the maximum number of routes allowed for a VRF exceeds the threshold. However, additional routes are still allowed.

Defaults

No default behavior or values.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

To use the **maximum routes** command, you must enter the VRF configuration submode. In this submode you create a VRF routing table and assign a route distinguisher in one of the following formats:

- 16-bit autonomous system number (ASN): your 32-bit number. For example, 101.
- 32-bit address: your 16-bit number. For example, 192.168.255.255.

You then create a route-target extended community for a VRF and specify the import, export, or both arguments for the **route-target** command. These arguments allow you to configure a router to import and export routing information to the target VPN extended community.

Examples

In the following example, the route distinguisher ASN is 100, and the maximum number of VRF routes to allow is set to 1000. When the maximum routes for the VRF reaches 1000, the router issues a syslog error message, but continues to accept new VRF routes.

```
ip vrf vrf1
 rd 100:1
 route-target import 100:1
 maximum routes 1000 warn-only
```

Related Commands

Command	Description
import map	Configures an import route map for a specified VRF for more control over routes imported into the VRF.
rd	Creates VRF routing and forwarding tables and specifies the default route distinguisher for a VPN.
route-target	Configures a VRF route target community for importing and exporting extended community attributes.

metric-style narrow

To configure a router running IS-IS so that it generates and accepts old-style type, length, and value objects (TLVs), use the **metric-style narrow** router configuration command. To disable this feature, 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 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.

Examples

In the following example, the router is instructed 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 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** router configuration command. To disable this feature, 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 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.

Examples

In the following example, a router is configured 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 IS-IS so that it generates and accepts only new-style type, length, and value objects (TLVs), use the **metric-style wide** router configuration command. To disable this feature, 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 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
Release 12.0(5)S	This command was introduced.

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

In the following example, a router is configured 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 rp ip

To enable Multilayer Switching Protocol (MLSP), use the **mls rp ip** command in global configuration mode. To disable MLS, use the **no** form of this command.

mls rp ip

no mls rp ip

Syntax Description

There are no arguments or keywords for this command.

Defaults

The default is MLS disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Usage Guidelines

Use this command to enable MLS, either globally or on a specific interface. MLSP is the protocol that runs between the switches and routers.

Examples

The following example enables MLS:

```
mls rp ip
```

Related Commands

Command	Description
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp nde-address	Specifies a NetFlow Data Export address.
mls rp vlan-id	Assigns a VLAN ID.
mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a VTP domain.
show mls rp	Displays MLS details, including specifics for MLSP.
show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

mls rp ip multicast

To enable IP multicast Multilayer Switching (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000, use the **mls rp ip multicast** command in interface configuration mode. To disable IP multicast Multilayer Switching (MLS) on the interface or VLAN, use the **no** form of this command.

mls rp ip multicast

no mls rp ip multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This feature is available only on specific router platforms connected to a Catalyst 5000 switch. Use this feature to reduce multicast load on the router. The switch will perform the multicast packet replication and forwarding.

IP multicast MLS is enabled by default on an interface once IP multicast routing and PIM are enabled.

Examples

The following example disables IP multicast MLS:

```
interface fastethernet1/0.1
 no mls rp ip multicast
```

Related Commands

Command	Description
mls rp ip multicast management-interface	Assigns a different interface (other than the default) to act as the management interface for MLSP.
show ip mroute	Displays the contents of the IP multicast routing table.
show mls rp interface	Displays hardware-switched multicast flow information about IP multicast MLS.

mls rp ip multicast management-interface

To assign a different interface (other than the default) to act as the management interface for Multilayer Switching Protocol (MLSP), use the **mls rp ip multicast management-interface** command in interface configuration mode. To restore the default interface as the management interface, use the **no** form of this command.

mls rp ip multicast management-interface

no mls rp ip multicast management-interface

Syntax Description

This command has no arguments or keywords.

Defaults

When IP multicast MLS is enabled, the subinterface (or VLAN interface) that has the lowest VLAN ID and is active (in the "up" state) is automatically selected as the management interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

When you enable IP multicast MLS, the subinterface (or VLAN interface) that has the lowest VLAN ID and is active (in the "up" state) is automatically selected as the *management interface*. The one-hop protocol MLSP is used between a router and a switch to pass messages about hardware-switched flows. MLSP packets are sent and received on the management interface. Typically, the interface in VLAN 1 is chosen (if that interface exists). Only one management interface is allowed on a single trunk link.

In most cases, we recommend that the management interface be determined by default. However, you can optionally use this command to specify a different router interface or subinterface as the management interface. We recommend using a subinterface with minimal data traffic so that multicast MLSP packets can be sent and received more quickly.

If the user-configured management interface goes down, the router uses the default interface (the active interface with the lowest VLAN ID) until the user-configured interface comes up again.

Examples

The following example configures the Fast Ethernet interface as the management interface:

```
interface fastethernet1/0.1
 mls rp ip multicast management-interface
```

Related Commands

Command	Description
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.

mls rp ipx (global)

To enable the router as an IPX Multilayer Switching (MLS) Route Processor (RP), use the **mls rp ipx** command in global configuration. To disable IPX MLS on the router, use the **no** form of this command.

mls rp ipx

no mls rp ipx

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Multilayer Switching Protocol (MLSP) is the protocol that runs between the MLS Switching Engine and the MLS RP.

Examples

The following example enables IPX MLS on the MLS RP:

```
mls rp ipx
```

Related Commands

Command	Description
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp ipx (interface)

To enable IPX MLS on a router interface, use the **mls rp ipx** command in interface configuration mode. To disable IPX MLS on a router interface, use the **no** form of this command.

mls rp ipx

no mls rp ipx

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(5)T	This command was introduced.

Usage Guidelines

Multilayer Switching Protocol (MLSP) is the protocol that runs between the MLS Switching Engine and the MLS RP.

Examples

The following example enables IPX MLS on a router interface:

```
mls rp ipx
```

Related Commands

Command	Description
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp locate ipx

To display information about all switches currently shortcutting for the specified IPX flows, use the **mls rp locate ipx** command in privileged EXEC mode.

mls rp locate ipx *destination-network.destination-node* [*source-network*]

Syntax Description

destination-network.destination-node	The destination network and destination node of IPX packet flows. The destination network consists of 1 to 8 hexadecimal numbers in the format xxxxxxxx. The destination node consists of 1 to 12 hexadecimal numbers in the format xxxx.xxxx.xxxx.
source-network	(Optional) The source network of the IPX flow. The source network consists of 1 to 8 hexadecimal numbers in the format yyyyyyyy.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

This example displays the switch that is shortcutting routed flows to the specified IPX flow:

```
mls rp locate ipx 30.0000.1111.2222
    locator response from switch id 0010.1400.601f
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp management-interface

To specify an interface as the management interface, use the **mls rp management-interface** command in interface configuration mode. To remove an interface as the management interface, use the **no** form of this command.

mls rp management-interface

no mls rp management-interface

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Usage Guidelines

Multilayer Switching Protocol (MLSP) packets are sent and received through the management interface.

Select only one IPX Multilayer Switching (MLS) interface connected to the switch. If you fail to select this interface, no connection between the MLS Route Processor (RP) and the MLS Switching Engine will occur, and any routing updates or changes to access lists will not be reflected on the switch.

Examples

The following example selects a management interface:

```
mls rp management-interface
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp nde-address

To specify a NetFlow Data Export address, use the **mls rp nde-address** command in global configuration mode.

mls rp nde-address *ip-address*

Syntax Description

ip-address	NDE IP address.

Defaults

No default behaviors or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Usage Guidelines

Use this command on an RP to specify the NetFlow Data Export address for a router. If you *do not* specify an NDE IP address for the MLS RP, the MLS RP automatically selects one of its interface's IP addresses and uses that IP address as its NDE IP address *and* its MLS IP address.

Examples

The following example sets the NDE address to 170.25.2.1:

```
mls rp nde-address 170.25.2.1
```

Related Commands

Command	Description
mls rp ip	Enables MLSP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN ID.
mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a VTP domain.
show mls rp	Displays MLS details, including specifics for MLSP.
show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

mls rp vlan-id

To assign a virtual LAN (VLAN) identification number to an IPX MLS interface, use the **mls rp vlan-id** command in interface configuration mode. To remove a VLAN identification number, use the **no** form of this command.

mls rp vlan-id *vlan-id-number*

no mls rp vlan-id *vlan-id-number*

Syntax Description

vlan-id-number	A VLAN identification number from 1 to 4096.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Usage Guidelines

The assigned IPX MLS interface must be either an Ethernet or Fast Ethernet interface—both without subinterfaces.

Examples

The following example assigns the VLAN identification number 23 to an IPX MLS interface:

```
mls rp vlan-id 23
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp vtp-domain

To assign a Multilayer Switching (MLS) interface to a specific Virtual Trunk Protocol (VTP) domain on the MLS Route Processor (RP), use the **mls rp vtp-domain** command in interface configuration mode. To remove a VTP domain, use the **no** form of this command.

mls rp vtp-domain *domain-name*

no mls rp vtp-domain *domain-name*

Syntax Description

domain-name	The name of the VTP domain assigned to an MLS interface and its related switches.

Defaults

The interface is assigned to the null domain.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Usage Guidelines

The assigned IPX MLS interface must be either an Ethernet or Fast Ethernet interface—both without subinterfaces.

Examples

The following example assigns the MLS interface to the VTP domain named engineering:

```
mls rp vtp-domain engineering
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mpls atm control-vc

To configure the VPI and VCI to be used for the initial link to the label switching peer device, use the **mpls atm control-vc** interface configuration command. To clear the interface configuration, 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.
vci	Virtual channel identifier.

Defaults

If the subinterface has not changed to a VP tunnel, the default is 0/32. If the subinterface corresponds to VP tunnel VPI X, the default is X/32.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
12.1(3)T	This command was modified to reflect new MPLS IETF terminology.

Usage Guidelines

The initial link is used to establish the TDP session and to carry non-IP traffic. For a router interface (for example, an AIP), ATM label switching can be enabled only on a label-switch 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.

On the Cisco LightStream 1010 ATM switch, a subinterface corresponds to a VP tunnel; thus, the entry in the VPI field of the control-vc must match the entry in the VPI field of the VP tunnel.

Examples

The following commands create a label switching subinterface on a router and select VPI 1 and VCI 34 as the control VC:

```
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
show mpls interfaces	Displays information about one or more interfaces for which label switching has been enabled.

mpls atm vpi

To configure the range of values to be used in the VPI field for label VCs, use the **mpls atm vpi** interface configuration command. To clear the interface configuration, use the **no** form of this command.

mpls atm vpi *vpi* [**-** *vpi*]

no mpls atm vpi *vpi* [**-** *vpi*]

Syntax Description

vpi	Virtual path identifier (low end of range).
- *vpi*	(Optional) Virtual path identifier (high end of range).

Defaults

The default is 1-1.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
12.1(3)T	This command was modified to reflect new MPLS IETF terminology.

Usage Guidelines

To configure ATM label switching on a router interface (for example, an ATM interface processor), you must enable a label switching subinterface.

Note The **mpls atm control-vc** and **mpls atm vpi** interface 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 (overlapping of labels in common) of the range configured at each end of the connection.

Examples

In the following example, a subinterface is created and a VPI range from 1 to 3 is selected:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm vpi 1-3
```

Related Commands

Command	Description
mpls atm control-vc	Configures the VPI and VCI to be used for the initial link to the label switching peer device.

mpls ip (global configuration)

To enable MPLS forwarding of IPv4 packets along normally routed paths for the platform, use the **mpls ip** global configuration command. 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
12.1(3)T	This command was introduced.

Usage Guidelines

This command enables MPLS forwarding of IPv4 packets along normally routed paths (sometimes called dynamic label switching). For a given interface to perform dynamic label switching, this function must be enabled for the interface and 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 TSP tunnels.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label VCs originating at, terminating at, or passing through the platform.

Examples

In the following example, dynamic label switching is disabled for the platform, terminating all label distribution for the platform:

```
Router(config)# no mpls ip
```

Related Commands

Command	Description
mpls ip (interface configuration)	Enables label switching of IPv4 packets along normally routed paths for the associated interface.

mpls ip (interface configuration)

To enable MPLS forwarding of IPv4 packets along normally routed paths for a particular interface, use the **mpls ip** interface configuration command. 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

MPLS forwarding of IPv4 packets along normally routed paths for the interface is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

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, you can start label distribution for the interface by initiating 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; it also ends label distribution for the interface. The **no** form of this command does not affect the sending of labeled packets through any TSP tunnels that might use the interface.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label VCs beginning at, terminating at, or passing through the interface.

Examples

In the following example, label switching is enabled on Ethernet interface o/2:

```
Router(config)# configure terminal
Router(config-if)# interface e0/2
Router(config-if)# mpls ip
```

Related Commands

Command	Description
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** global configuration command.

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
11.1 CT	This command was introduced.
12.1(3)T	This command was modified to reflect new MPLS IETF terminology.

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 commands 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 propagate-ttl

To control the generation of the time to live (TTL) field in the MPLS header when labels are first added to an IP packet, use the **mpls ip propagate-ttl** global configuration command. 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

By default, 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.

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 forward** 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

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** privileged EXEC command. To disable this feature, use the **no** form of the 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

By default, 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.

12.0 S	Packets are forwarded through the use of the global routing table.
12.0 ST	Packets are forwarded through the use of the original label stack.
12.1 T	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.

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.)

Related Commands

Command	Description
traceroute	Displays the routes that packets take through a network to their destinations.

mpls label range

To configure the range of local labels available for use on packet interfaces, use the **mpls label range** global configuration command. To revert to the platform defaults, use the **no** form of this command.

mpls label range *min max*

no mpls label range

Syntax Description

min	The smallest label allowed in the label space. The default is 16.
max	The largest label allowed in the label space. The default is 1048575.

Defaults

min: 16

max: 1048575

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 MPLS IETF terminology and CLI command syntax.

Usage Guidelines

The labels 0 through 15 are reserved by the IETF (see draft-ietf-mpls-label-encaps-07.txt for details) and cannot be included in the range specified by the **mpls label range** 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 VPNs, and so on).

If you specify a new label range that does not overlap the range currently in use, the new range will not take effect until the router is reloaded again.

Examples

The following example configures the size of the local label space. In this example, the *min* argument is set with the value of 200, and the *max* value is set with the value of 120000. Because the new range does not overlap the current label range (assumed to be the default, that is, the *min* argument of 16 and the *max* argument of 100000), the new range will not take effect until the router is reloaded.

```
Router# configure terminal
Router(config)# mpls label range 200 120000
% Label range changes will take effect at the next reload.
Router(config)#
```

If you had specified a new range that overlaps the current range (for example, new range of the *min* argument of 16 and the *max* argument of 120000), then the new range would take effect immediately.

Related Commands

Command	Description
show mpls label range	Displays the range of the MPLS local label space.

mpls mtu

To set the per-interface Multiprotocol Label Switching (MPLS) maximum transmission unit (MTU) for labeled packets, use the **mpls mtu** interface configuration command. To restore the default, use the **no** form of this command.

mpls mtu *bytes*

no mpls mtu

Syntax Description

bytes	The MTU in bytes includes the label stack in the value. For example, to transport an IPv4 packet of 1500 bytes from the edge through an MPLS core, you need an MPLS MTU of at least 1504 bytes. This value accounts for the single 4-byte label and avoids fragmentation. Use the following calculation to determine the MTU: MPLS MTU = edge MTU + (label stack * 4 bytes)

Defaults

The default MPLS MTU is the MTU configured for the interface. The minimum allowable value is 64; the maximum allowable value is interface dependent.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CT	This command was introduced.
12.1(3)T	This command was modified to reflect new MPLS IETF terminology.

Usage Guidelines

- MPLS baby giant packets (packets that were larger than the interface MTU value should allow) are no longer supported. Therefore, the MPLS MTU value cannot be larger than the interface MTU value.

Note The MPLS MTU setting is displayed in the **show running-config** command output only if the MPLS MTU value is different from the interface MTU value.

- 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 values for the interfaces on each side of a link must be equal for OSPF adjacencies to come up.
- 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.
- 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.
- The migration path for configurations using an MPLS MTU value greater than the interface MTU value is as follows:
  - During system initialization the system attempts to automatically set the interface MTU value to the configured MPLS MTU value.
  - If you attempt to set the MPLS MTU to a value larger than that of the interface MTU when the system is *not* doing its initial configuration, there is an error message indicating that you must increase the interface MTU value before you can set the MPLS MTU value.

Examples

The following example sets the maximum labeled packet size for the Fastethernet interface to 1508, which is common in an MPLS core carrying MPLS VPN traffic, for example:

```
interface Fastethernet0
  mpls mtu 1508
```

mpls netflow egress

To enable MPLS egress NetFlow accounting on an interface, use the **mpls netflow egress** interface configuration command. 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.

Defaults

No default behavior or values.

Command Modes

Interface configuration

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.

Usage Guidelines

Use this command to configure the PE-CE interface of a PE router.

Examples

In the following example, MPLS egress NetFlow accounting is enabled on the egress PE interface that connects to the CE interface at the destination 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. If MPLS egress NetFlow accounting is enabled on an interface, the value is any number other than 0. If MPLS egress NetFlow accounting is disabled on an interface, the value is 0.

mpls traffic-eng

To configure a router running IS-IS so that it floods MPLS traffic engineering link information into the indicated IS-IS level, use the **mpls traffic-eng** router configuration command. To disable this feature, 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 traffic engineering link information into IS-IS level 1.
level-2	Floods MPLS traffic engineering link information into IS-IS level 2.

Defaults

Flooding is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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

In the following example, MPLS traffic engineering is turned on 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** interface configuration command. To disable this feature, 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.

Defaults

IGP cost of the link.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the IGP cost of the link is overridden, and the cost is set 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) MPLS so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** router configuration command. To disable this feature, use the **no** form of this command.

mpls traffic-eng area *num*

no mpls traffic-eng area *num*

Syntax Description

num	The OSPF area on which MPLS traffic engineering is enabled.

Defaults

No default behavior or values.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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

In the following example, a router running OSPF MPLS is configured 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 attribute-flags

To set the user-specified attribute flags for the interface, use the **mpls traffic-eng attribute-flags** interface configuration command. To disable this feature, use the **no** form of this command.

mpls traffic-eng attribute-flags *attributes*

no mpls traffic-eng attribute-flags

Syntax Description

attributes	Links 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.

Defaults

0x0

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

This command assigns attributes to a link so that tunnels with matching attributes (represented by their affinity bits) prefer this link instead of 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

In the following example, the attribute flags are set 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 flooding thresholds

To set a link's reserved bandwidth thresholds, use the **mpls traffic-eng flooding thresholds** interface configuration command. 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 resource availability.
up	Sets the thresholds for increased resource availability.
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.

The default for **down** is 100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, 15.

The default for **up** is 15, 30, 45, 60, 75, 80, 85, 90, 95, 97, 98, 99, 100.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

When a threshold is crossed, MPLS traffic engineering link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding was disabled.

Examples

In the following example, the link's reserved bandwidth is set for decreased resource availability (down) and for increased resource availability (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 OSPF to advertise an MPLS Traffic Engineering (TE) interface to area 0, use the **mpls traffic-eng interface** command in router configuration mode. To remove the interface from area 0, use the **no** form of this command.

mpls traffic-eng interface *interface* **area** *area*

no mpls traffic-eng interface *interface* **area** *area*

Syntax Description

interface	The interface where the virtual link exists.
area	The area where the link should be advertised. This is generally area 0.

Defaults

No default behaviors.

Command Modes

Router configuration

Command History

Release	Modification
12.0(11)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This command is useful in MPLS TE configurations that use virtual links between Area Border Routers (ABRs) with OSPF.

Often, OSPF ABRs have a link between them which is in a non-zero area, and a virtual link that in effect puts that link into area 0 as well as the non-zero area. This command allows you to advertise the link between ABRs into area 0, even though the link is in a non-zero area. This solves for TE the same problem that virtual links solve for IP routing.

Examples

In the following example, OSPF announces interface pos0/0 to area 0:

```
Router(config)# router ospf 1
Router(config-router)# mpls traffic-eng interface pos0/0 area 0
```

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** router configuration command. To disable this feature, 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

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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** router configuration command. To disable this feature, 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

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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

In the following example, the interval length for periodic flooding is set 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 link timers bandwidth-hold

To set the length of time that bandwidth is "held" for a 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.

Examples

The following example sets the length of time that bandwidth is held to 10 seconds.

```
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

3 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

Use this command to set the interval for periodic flooding of TE topology information.

Changes in the 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.

```
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 logging lsp

To log certain traffic engineering label-switched path (LSP) events, use the **mpls traffic-eng logging lsp** router configuration command. To disable this feature, use the **no** form of this command.

mpls traffic-eng logging lsp {**path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns**}[*aclnum*]

no mpls traffic-eng logging lsp {**path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns**}[*aclnum*]

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.
aclnum	(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

Router configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, path errors are logged 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** router configuration command. To disable this feature, use the **no** form of this command.

mpls traffic-eng logging tunnel lsp-selection [*aclnum*]

no mpls traffic-eng logging tunnel lsp-selection [*aclnum*]

Syntax Description

lsp-selection	Logs events related to the selection of an LSP for a traffic engineering tunnel.
aclnum	(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

Router configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, traffic engineering tunnel events associated with access list 3 are logged:

```
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 reoptimize

To force immediate reoptimization of all traffic engineering tunnels, use the **mpls traffic-eng reoptimize** EXEC command.

mpls traffic-eng reoptimize

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples

In the following example, all traffic engineering tunnels are immediately reoptimized:

```
Router2# mpls traffic-eng reoptimize
```

mpls traffic-eng reoptimize events

To turn on automatic reoptimization of MPLS traffic engineering when certain events occur, such as when an interface becomes operational, use the **mpls traffic-eng reoptimize events** router configuration command. To disable this feature, 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

Router configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, automatic reoptimization is turned on 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 (EXEC mode)	Reoptimizes all traffic engineering tunnels immediately.

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** router configuration command. To disable this feature, 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.

Defaults

3600 seconds (1 hour), with a range of 0 to 604800 seconds (1 week)

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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 signalling is successful, the device replaces the old, inferior LSP with the new, better LSP.

Examples

In the following example, the reoptimization frequency is set to 1 day:

```
Router(config)# mpls traffic-eng reoptimize timers frequency 86400
```

Related Commands

Command	Description
tunnel mpls traffic-eng path-option	If **lockdown** is specified, does not do a reoptimization check on this tunnel.
mpls traffic-eng reoptimize (EXEC mode)	Reoptimizes all traffic engineering tunnels immediately.

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** router configuration command. To disable this feature, 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 default behavior or values.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

This router's 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 destination node's traffic engineering router identifier, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.

Examples

In the following example, the traffic engineering router identifier is specified 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 signalling advertise implicit-null

To use MPLS encoding for the implicit-null label in signalling messages sent to neighbors that match the specified access list, use the **mpls traffic-eng signalling advertise implicit-null** router configuration command. To disable this feature, use the **no** form of this command.

mpls traffic-eng signalling advertise implicit-null [*aclname* | *aclnum*]

no mpls traffic-eng signalling advertise implicit-null

Syntax Description

aclname	Name of the access list.
aclnum	Number of the access list.

Defaults

Use the Cisco encoding for the implicit-null label in signalling messages.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples

In the following example, the router is configured to use MPLS encoding for the implicit-null label when it sends signalling messages to certain peers:

```
Router(config)# mpls traffic-eng signalling advertise implicit-null
```

mpls traffic-eng tunnels (global)

To enable MPLS traffic engineering tunnel signaling on a device, use the **mpls traffic-eng tunnels** global configuration command. To disable this feature, 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 feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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

In the following example, MPLS traffic engineering tunnel signalling is turned on:

```
Router(config)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signalling on an interface.

mpls traffic-eng tunnels (interface)

To enable MPLS traffic engineering tunnel signalling on an interface (assuming that it is enabled on the device), use the **mpls traffic-eng tunnels** interface configuration command. To disable this feature, 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 feature is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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 signalling requests.

Examples

In the following example, MPLS traffic engineering is enabled on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
mpls traffic-eng tunnels (global)	Enables MPLS traffic engineering tunnel signalling on a device.

mpoa client config name

To define an MPC with a specified name, use the **mpoa client config name** command in global configuration mode. To delete the MPC, use the **no** form of this command.

mpoa client config name *mpc-name*

no mpoa client config name *mpc-name*

Syntax Description

mpc-name	Specifies the name of an MPC.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

When you configure or create an MPC, you automatically enter the MPC configuration mode. From here, you can enter subcommands to define or change MPC variables specific only to this MPC. Note that the MPC is not functional until it is attached to a hardware interface.

Examples

The following example creates or modifies the MPC named ip_mpc:

```
mpoa client config name ip_mpc
```

Related Commands

Command	Description
atm-address	Overrides the control ATM address of an MPC or MPS.
shortcut-frame-count	Specifies the maximum number of times a packet can be routed to the default router within shortcut-frame time before an MPOA resolution request is sent.
shortcut-frame-time	Sets the shortcut-setup frame time (in seconds) for the MPC.

mpoa client name

To attach an MPC to a major ATM interface, use the **mpoa client name** command in interface configuration mode. To break the attachment, use the **no** form of this command.

mpoa client name *mpc-name*

no mpoa client name *mpc-name*

Syntax Description

mpc-name	Specifies the name of an MPC.

Defaults

No MPC is attached to an ATM interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

The **mpoa client name** command provides an interface to the MPC through which the MPC can set up and receive calls.

When you enter this command on a major interface that is up and operational, the named MPC becomes operational. Once the MPC is fully operational, it can register its ATM address.

Examples

The following example attaches the MPC named ip_mpc to an interface:

```
interface atm 1/0
 mpoa client name ip_mpc
```

mpoa server config name

To define an MPS with the specified name, use the **mpoa server config name** command in global configuration mode. To delete an MPS, use the **no** form of this command.

mpoa server config name *mps-name*

no mpoa server config name *mps-name*

Syntax Description

mps-name	Name of the MPOA server.

Defaults

No MPS is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

This command defines an MPS with the specified name. The MPS does not actually start functioning until it is attached to a specific hardware interface. Once that attachment is complete, the MPS starts functioning. When you configure or create an MPS, you automatically enter the MPS configuration mode.

You can define the MPS variables specific to an MPS only after that MPS has been defined with a specified name. After this command is entered, further commands can be used to change MPS variables that are specific only to this MPS.

Examples

The following example defines the MPS named MYMPS:

```
mpoa server config name MYMPS
```

mpoa server name

To attach an MPS to a major ATM interface, use the **mpoa server name** command in interface configuration mode. To break the attachment, use the **no** form of this command.

mpoa server name *mps-name*

no mpoa server name *mps-name*

Syntax Description

mps-name	Name of the MPOA server.

Defaults

No MPS is attached to an ATM interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

This command attaches an MPS to a specific (major) interface. At this point, the MPS can obtain its autogenerated ATM address and an interface through which it can communicate to the neighboring MPOA devices. Only when an MPS is both defined globally and attached to an interface is it considered to be operational. Although multiple different servers may share the same hardware interface, an MPS can be attached to only a single interface at any one time. Note that the specified MPS must have already been defined when this command is entered.

Examples

The following example attaches the MPS named MYMPS to an ATM interface:

```
mpoa server name MYMPS
```

mpoa server name trigger ip-address

To originate an MPOA trigger for the specified IP address to the specified MPOA client from the specified MPS, use the **mpoa server name trigger ip-address** interface configuration command.

mpoa server name *mps-name* **trigger ip-address** *ip address* [**mpc-address** *mpc-address*]

Syntax Description

mps-name	Specifies the name of the MPOA server.
ip address	Specifies the IP address.
mpc-address *mpc-address*	(Optional) Specifies the MPOA client (MPC) address to which the trigger should be sent. If the address is not specified, a trigger will be sent to all clients.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

This command sends an MPOA trigger for the specified IP address to the specified MPOA client from the specified MPOA server. If an MPOA client is not specified, it is triggered to all MPOA clients.

Examples

The following example sends an MPOA trigger for the specified IP address 128.9.0.7 to all known MPOA clients from the MPOA server named MYMPS:

```
mpoa server name MYMPS trigger ip-address 128.9.0.7
```

name elan-id

To configure the emulated LAN (ELAN) ID of an ELAN in the LECS database to participate in MPOA, use the **name elan-id** command in LANE database configuration mode. To disable the ELAN ID of an ELAN in the LECS database to participate in MPOA, use the **no** form of this command.

name *name* **elan-id** *id*

no name *name* **elan-id** *id*

Syntax Description

name	Specifies the name of the ELAN.
id	Specifies the identification number of the ELAN.

Defaults

No ELAN ID is configured.

Command Modes

LANE database configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

To participate in MPOA, a LEC must have an ELAN ID. The LEC obtains the ELAN ID from the LECS. In case the LEC bypasses the LECS phase, the LEC can get the ELAN ID from the LES when the **name elan-id** command is used.

Examples

The following example sets the ELAN ID to 10 for an ELAN named MYELAN:

```
name MYELAN elan-id 10
```

Related Commands

Command	Description
lane server-bus	Enables a LANE server and a broadcast and unknown server on the specified subinterface with the ELAN ID.

name local-seg-id

To specify or replace the ring number of the emulated LAN (ELAN) in the configuration server's configuration database, use the **name local-seg-id** command in database configuration mode. To remove the ring number from the database, use the **no** form of this command.

name *elan-name* **local-seg-id** *segment-number*

no name *elan-name* **local-seg-id** *segment-number*

Syntax Description

elan-name	Name of the ELAN. The maximum length of the name is 32 characters.
segment-number	Segment number to be assigned to the ELAN. The number ranges from 1 to 4095.

Defaults

No ELAN name or segment number is provided.

Command Modes

Database configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is ordinarily used for Token Ring LANE.

The same LANE ring number cannot be assigned to more than one ELAN.

The **no** form of this command deletes the relationships.

Examples

The following example specifies a ring number of 1024 for the ELAN named red:

```
name red local-seg-id 1024
```

Related Commands

Command	Description
default-name	Provides an ELAN name in the database of the configuration server for those client MAC addresses and client ATM addresses that do not have explicit ELAN name bindings.
lane database	Creates a named configuration database that can be associated with a configuration server.
mac-address	Sets the MAC-layer address of the Cisco Token Ring.

name preempt

To set the emulated LAN (ELAN) preempt, use the **name preempt** command in LANE database configuration mode. To disable preemption, use the **no** form of this command.

name *elan-name* **preempt**

no name *elan-name* **preempt**

Syntax Description

elan-name	Specifies the name of the ELAN.

Defaults

Preemption is off by default.

Command Modes

LANE database configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

In prior releases, when the primary LES failed, the Cisco SSRP protocol switched over to a secondary LES. But when a LES that is ranked higher in the list came back up, the SSRP protocol switched the active LES to the new LES, which had a higher priority. This forced the network to flap multiple times. We have prevented the network flapping by staying with the currently active master LES regardless of the priority. If a higher priority LES comes back online, SSRP will not switch to that LES.

LES preemption is off by default. The first LES that comes on becomes the master. Users can revert to the old behavior (of switching to the higher-priority LES all the time) by specifying the **name** *elan-name* **preempt** command in the LECS database.

Examples

The following example sets the ELAN preempt for the ELAN named MYELAN:

```
name MYELAN preempt
```

name server-atm-address

To specify or replace the ATM address of the LANE server for the emulated LAN (ELAN) in the configuration server's configuration database, use the **name server-atm-address** command in database configuration mode. To remove it from the database, use the **no** form of this command.

name *elan-name* **server-atm-address** *atm-address* [**restricted | un-restricted**] [**index** *number*]

no name *elan-name* **server-atm-address** *atm-address* [**restricted | un-restricted**] [**index** *number*]

Syntax Description

elan-name	Name of the ELAN. Maximum length is 32 characters.
atm-address	LANE server's ATM address.
**restricted	un-restricted**	(Optional) Membership in the named ELAN is restricted to the LANE clients explicitly defined to the ELAN in the configuration server's database.
index *number*	(Optional) Priority number. When specifying multiple LANE servers for fault tolerance, you can specify a priority for each server. 0 is the highest priority.

Defaults

No emulated LAN name or server ATM address is provided.

Command Modes

Database configuration

Command History

Release	Modification
11.0	This command was introduced.
11.2	The following keywords were added: • **un-restricted** • **index**

Usage Guidelines

ELAN names must be unique within one named LANE configuration database.

Specifying an existing ELAN name with a new LANE server ATM address adds the LANE server ATM address for that ELAN for redundant server operation or simple LANE service replication. This command can be used multiple times.

The **no** form of this command deletes the relationships.

Examples

The following example configures the example3 database with two restricted and one unrestricted ELANs. The clients that can be assigned to the eng and mkt ELANs are specified using the **client-atm-address** commands. All other clients are assigned to the man ELAN.

```
lane database example3
 name eng server-atm-address 39.000001415555121101020304.0800.200c.1001.02 restricted
 name man server-atm-address 39.000001415555121101020304.0800.200c.1001.01
 name mkt server-atm-address 39.000001415555121101020304.0800.200c.4001.01 restricted
 client-atm-address 39.000001415555121101020304.0800.200c.1000.02 name eng
 client-atm-address 39.000001415555121101020304.0800.200c.2000.02 name eng
 client-atm-address 39.000001415555121101020304.0800.200c.3000.02 name mkt
 client-atm-address 39.000001415555121101020304.0800.200c.4000.01 name mkt
 default-name man
```

Related Commands

Command	Description
client-atm-address name	Adds a LANE client address entry to the configuration database of the configuration server.
default-name	Provides an ELAN name in the database of the configuration server for those client MAC addresses and client ATM addresses that do not have explicit ELAN name bindings.
lane database	Creates a named configuration database that can be associated with a configuration server.
mac-address	Sets the MAC-layer address of the Cisco Token Ring.

neighbor activate

To enable the exchange of information with a neighboring router, use the **neighbor activate** command in address family configuration or router configuration mode. To disable the exchange of an address with a neighboring router, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **activate**

no neighbor {*ip-address* | *peer-group-name*} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of BGP peer group.

Defaults

The exchange of addresses with neighbors is enabled by default for the IPv4 address family. You can disable IPv4 address exchange using the **no default bgp ipv4 activate** command, or you can disable it for a particular neighbor using the **no** form of the **neighbor activate** command.

For all other address families, address exchange is disabled by default. You can explicitly activate the default command using the appropriate address family configuration.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to enable or disable the exchange of addresses with a neighboring router.

Examples

The following example activates advertisement of NLRI for address family named VPN IPv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 144.0.0.44:

```
address-family vpnv4
neighbor PEPEER activate
neighbor 144.0.0.44 activate
exit-address-family
```

Related Commands

Command	Description
address-family	Enters the address family submode for configuring routing protocols, such as BGP, RIP, and static routing.
exit-address-family	Exits from the address family submode.

neighbor allowas-in

To configure PE routers to allow readvertisement of all prefixes containing duplicate ASNs, use the **neighbor allowas-in** command in router configuration mode. To disable the readvertisement of a PE router's ASN, use the **no** form of this command.

neighbor *ip-address* **allowas-in** [*number*]

no neighbor *ip-address* **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. Valid values are from 1 to 10. If no number is supplied, the default value of 3 times is used.

Defaults

No default behavior or values.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1	This command was integrated into Cicso IOS Release 12.1.
12.2	This command was integrated into Cicso IOS Release 12.2.

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 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

In the following example, the PE router with ASN 100 is configured to allow prefixes from the VRF address family 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 bgp 100
 address-family ipv4 vrf vrf1
 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 PE router to override the ASN of a site with the ASN of a provider, use the **neighbor as-override** command in router configuration mode. To remove 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

No default behavior or values.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

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 bgp 100
 neighbor 192.168.255.255 remote-as 109
 neighbor 192.168.255.255 update-source loopback0
 address-family ipv4 vrf vpn1
 neighbor 192.168.255.255 activate
 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.

network-id

To specify the network ID of an MPS, use the **network-id** command in MPS configuration mode. To revert to the default value (default value is 1), use the **no** form of this command.

network-id *id*

no network-*id*

Syntax Description

id	Specifies the network ID of the MPOA server.

Defaults

The default value for the network id is 1.

Command Modes

MPS configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

Specifies the network ID of this MPS. This value is used in a very similar way the NHRP network ID is used. It is for partitioning NBMA clouds artificially by administration.

Examples

The following example sets the network ID to 5:

```
network-id 5
```

next-address

To specify the next IP address in the explicit path, use the **next-address** IP explicit path configuration command. To disable this feature, use the **no** form of this command.

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

no next-address *A.B.C.D*

Syntax Description

A.B.C.D	Next IP address in the explicit path.

Defaults

No default behavior or values.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the number 60 is assigned to the IP explicit path, the path is enabled, and 3.3.27.3 is specified 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 3.3.27.3

Explicit Path identifier 60:
    1: next-address 3.3.27.3
Router(cfg-ip-exp1-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 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.

rate-limit

To configure CAR and DCAR policies, use the **rate-limit** interface configuration command. To remove the rate limit from the configuration, use the **no** form of this command.

rate-limit {**input** | **output**} [**access-group** [**rate-limit**] *acl-index*] *bps*
burst-normal burst-max **conform-action** *conform-action* **exceed-action** *exceed-action*

no rate-limit {**input** | **output**}[**access-group** [**rate-limit**] *acl-index*] *bps*
burst-normal burst-max **conform-action** *conform-action* **exceed-action** *exceed-action*

Syntax Description

input	Applies this CAR traffic policy to packets received on this input interface.
output	Applies this CAR traffic policy to packets sent on this output interface.
access-group	(Optional) Applies this CAR traffic policy to the specified access list.
rate-limit	(Optional) The access list is a rate-limit access list.
acl-index	(Optional) Access list number.
bps	Average rate (in bits per second). The value must be in increments of 8 kbps.
burst-normal	Normal burst size (in bytes). The minimum value is bits per second divided by 2000.
burst-max	Excess burst size (in bytes).
conform-action *conform-action*	Action to take on packets that conform to the specified rate limit. Specify one of the following keywords: • **continue**—Evaluates the next **rate-limit** command. • **drop**—Drops the packet. • **set-dscp-continue**—Sets the differentiated services code point (DSCP) (0 to 63) and evaluate the next **rate-limit** command. • **set-dscp-transmit**—Sends the DSCP and transmit the packet. • **set-mpls-exp-continue**—Sets the MPLS experimental bits (0 to 7) and evaluates the next **rate-limit** command. • **set-mpls-exp-transmit**—Sets the MPLS experimental bits (0 to 7) and sends the packet. • **set-prec-continue**—Sets the IP precedence (0 to 7) and evaluates the next **rate-limit** command. • **set-prec-transmit**—Sets the IP precedence (0 to 7) and sends the packet. • **set-qos-continue**—Sets the QoS group ID (1 to 99) and evaluates the next **rate-limit** command. • **set-qos-transmit**—Sets the QoS group ID (1 to 99) and sends the packet. • **transmit**—Sends the packet.

exceed-action *exceed-action*	Action to take on packets that exceed the specified rate limit. Specify one of the following keywords: • **continue**—Evaluates the next **rate-limit** command. • **drop**—Drops the packet. • **set-dscp-continue**—Sets the DSCP (0 to 63) and evaluates the next **rate-limit** command. • **set-dscp-transmit**—Sends the DSCP and sends the packet. • **set-mpls-exp-continue**—Sets the MPLS experimental bits (0 to 7) and evaluates the next **rate-limit** command. • **set-mpls-exp-transmit**—Sets the MPLS experimental bits (0 to 7) and sends the packet. • **set-prec-continue**—Sets the IP precedence (0 to 7) and evaluates the next **rate-limit** command. • **set-prec-transmit**—Sets the IP precedence (0 to 7) and sends the packet. • **set-qos-continue**—Sets the QoS group ID (1 to 99) and evaluates the next **rate-limit** command. • **set-qos-transmit**—Sets the QoS group ID (1 to 99) and sends the packet. • **transmit**—Sends the packet.

Defaults

CAR and DCAR are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.1(5)T	The **conform** and **exceed** actions were added for the MPLS experimental field.

Usage Guidelines

Use this command to configure your CAR policy on an interface. To specify multiple policies, enter this command once for each policy.

CAR and DCAR can be configured on an interface or subinterface.

Examples

In the following example, the rate is limited by application:

- All World Wide Web traffic is sent. However, the MPLS experimental field for web traffic that conforms to the first rate policy is set to 5. For nonconforming traffic, the IP precedence is set to 0 (best effort). See the following commands in the example:

```
rate-limit input rate-limit access-group 101 20000000 24000 32000 conform-action
set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0

access-list 101 permit tcp any any eq www
```

- FTP traffic is sent with an MPLS experimental field of 5 if it conforms to the second rate policy. If the FTP traffic exceeds the rate policy, it is dropped. See the following commands in the example:

```
rate-limit input access-group 102 10000000 24000 32000
conform-action set-mpls-exp-transmit 5 exceed-action drop

access-list 102 permit tcp any any eq ftp
```

- Any remaining traffic is limited to 8 Mbps, with a normal burst size of 16,000 bytes and an excess burst size of 24000 bytes. Traffic that conforms is sent with an MPLS experimental field of 5. Traffic that does not conform is dropped. See the following command in the example:

```
rate-limit input 8000000 16000 24000 conform-action set-mpls-exp-transmit 5
exceed-action drop
```

Notice that two access lists are created to classify the web and FTP traffic so that they can be handled separately by the CAR feature:

```
router(config)# interface Hssi0/0/0
router(config-if)# description 45Mbps to R2
router(config-if)# rate-limit input rate-limit access-group 101 20000000 24000 32000
  conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
router(config-if)# rate-limit input access-group 102 10000000 24000 32000
  conform-action set-mpls-exp-transmit 5 exceed-action drop
router(config-if)# rate-limit input 8000000 16000 24000 conform-action
  set-mpls-exp-transmit 5 exceed-action drop
router(config-if)# ip address 200.200.14.250 255.255.255.252
!
router(config-if)# access-list 101 permit tcp any any eq www
router(config-if)# access-list 102 permit tcp any any eq ftp
```

In the following example, the MPLS experimental field is set and the packet is sent:

```
router(config)# interface FastEtheret1/1/0
router(config)# rate-limit input 8000 1000 1000 access-group conform-action
  set mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 5
```

Related Commands

Command	Description
access-list rate-limit	Configures an access list for use with CAR policies.
show access-list rate-limit	Displays information about rate-limit access lists.
show interfaces rate-limit	Displays information about CAR for a specified interface.

rd

To create routing and forwarding tables for a VRF, 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.

Defaults

There is no default. A route distinguisher (RD) must be configured for a VRF to be functional.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

A 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.

Either RD is an ASN-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

*16-bit AS 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 configures a default RD for two VRFs. It illustrates the use of both AS-relative and IP-address-relative RDs:

```
ip vrf vrf_blue
rd 100:3
ip vrf vrf_red
173.13.0.12:200
```

Related Commands

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

route-target

To create a route-target extended community for a VRF, 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.

Defaults

There are no defaults. A VRF has no route-target extended community attributes associated with it until specified by the **route-target** command.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

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 BGP, 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 AS 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 route-target extended community attributes for a VRF. The result of the command sequence is that VRF named *vrf_blue* has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 173.27.0.130:200).

```
ip vrf vrf_blue
route-target both 1000:1
route-target export 1000:2
route-target import 173.27.0.130:200
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
import map	Configures an import route map for a VRF.

set ip next-hop verify-availability

To configure policy routing to verify that the next hops of a route map is a CDP neighbor before policy routing to that next hop, use the **set ip next-hop verify-availability** route-map configuration command.

set ip next-hop verify-availability

Syntax Description

This command has no arguments or keywords.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

This command might be used in a case such as you have some traffic traveling via a satellite to a next hop. It might be prudent to verify that the next hop is reachable before trying to policy route to it.

This command has the following restrictions:

- It causes some performance degradation.
- CDP must be configured on the interface.
- The next hop must be a Cisco device with CDP enabled.
- It is supported in process switching and CEF policy routing, but not available in dCEF, because of the dependency of the CDP neighbor database.

If the router is policy routing packets to the next hop and the next hop happens to be down, the router will try unsuccessfully to use Address Resolution Protocol (ARP) for the next hop (which is down). This behavior will continue forever.

To prevent this situation from occurring, use this command to configure the router to first verify that the next hops of the route map are the router's CDP neighbors before routing to that next hop.

This command is optional because some media or encapsulations do not support CDP, or it may not be a Cisco device that is sending the router traffic.

If this command is set and the next hop is not a CDP neighbor, the router looks to the subsequent next hop, if there is one. If there is none, the packets simply are not policy routed.

If this command is not set, the packets either are successfully policy routed or remain forever unrouted.

If you want to selectively verify availability of only some next hops, you can configure different route map entries (under the same route map name) with different criteria (using access list matching or packet size matching), and use the **set ip next-hop verify-availability** command selectively.

Examples

The following example configures Policy Routing with CEF. Policy routing is configured to verify that next hop 50.0.0.8 of route map named test is a CDP neighbor before the router tries to policy route to it.

If the first packet is being policy routed via route map named test sequence 10, the subsequent packets of the same flow always take the same route map named test sequence 10, not route map named test sequence 20, because they all match or pass access list 1 check.

```
ip cef
interface ethernet0/0/1
 ip route-cache flow
 ip policy route-map test
route-map test permit 10
 match ip address 1
 set ip precedence priority
 set ip next-hop 50.0.0.8
 set ip next-hop verify-availability
route-map test permit 20
```

set mpls experimental

To configure a policy to set the MPLS experimental field within the modular QoS command-line interface (CLI), use the **set mpls experimental** policy-map configuration command. To disable the policy map, use the **no** form of this command.

set mpls experimental *value*

no set mpls experimental *value*

Syntax Description

value	Specifies the value used to set MPLS experimental bits defined by the policy map. Valid values are 0 to 7, and they can be space-delimited. For example, 3 4 7.

Defaults

No default behavior or values.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the policy map to set the MPLS experimental field when it is undesirable to modify the IP precedence field.

Examples

The following example specifies a policy map named out_pmap. The policy map comprises class maps. Class map mpls_2 matches packets with MPLS experimental field 2 and resets the MPLS experimental field to 3.

```
router(config)# class-map mpls_2
   match mpls experimental 2
router(config)# policy-map out_pmap
   class mpls_2
      set mpls experimental 3
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class specified.
policy-map	Creates a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or an output interface to be used as the service policy for that interface.

set ospf router-id

To set a separate OSPF router ID for each interface or subinterface on a PE router for each directly attached 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

No default behavior or values.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

To use this command, you must enable OSPF and create a routing process.

Examples

In the following example, the PE router IP address 192.168.0.0 is matched 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 vlan

To group ports into a virtual LAN (VLAN), use the **set vlan** command in privileged EXEC mode.

set vlan *vlan-number module/port*

set vlan *vlan-number* [**name** *name*] [**type** {**ethernet** | **fddi** | **fddinet** | **trcrf** | **trbrf**}] [**state** {**active** | **suspend**}] [**said** *said*] [**mtu** *mtu*] [**ring** *hex-ring-number*] [**decring** *decimal-ring-number*] [**bridge** *bridge-number*] [**parent** *vlan-number*] [**mode** {**srt** | **srb**}] [**stp** {**ieee** | **ibm** | **auto**}] [**translation** *vlan-number*] [**backupcrf** {**off** | **on**}] [**aremaxhop** *hop-count*] [**stemaxhop** *hop-count*]

Syntax Description

vlan-number	Number identifying the VLAN.
module	Number of the module. This argument is not valid when defining or configuring Token Ring Bridge Relay Functions (TRBRFs).
port	Number of the port on the module belonging to the VLAN; this argument does not apply to TRBRFs.
name *name*	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
type {**ethernet** | **fddi** | **fddinet** | **trcrf** | **trbrf**}	(Optional) Identifies the VLAN type. The default type is Ethernet.
state {**active** | **suspend**}	(Optional) Specifies whether the state of the VLAN is active or suspended. VLANs in suspended state do not pass packets. The default state is active.
said *said*	(Optional) Specifies the security association identifier. Possible values are 1 to 4294967294. The default is 100001 for VLAN1, 100002 for VLAN 2, 100003 for VLAN 3, and so on. This argument does not apply to Token Ring Concentrator Relay Functions (TRCRFs) or TRBRFs.
mtu *mtu*	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use. Possible values are 576 to 18190. The default is 1500 bytes.
ring *hex-ring-number*	(Optional) Specifies the logical ring number for Token Ring VLANs. Possible values are hexadecimal numbers 0x1 to 0xFFF. This argument is valid and required only when defining a TRCRF.
decring *decimal-ring-number*	(Optional) Specifies the logical ring number for Token Ring VLANs. Possible values are decimal numbers 1 to 4095. This argument is valid and required only when defining a TRCRF.
bridge *bridge-number*	(Optional) Specifies the identification number of the bridge. Possible values are hexadecimal numbers 0x1 to 0xF. For Token Ring VLANs, the default is 0F. This argument is not valid for TRCRFs.
parent *vlan-number*	(Optional) Sets a parent VLAN. The range for *vlan-number* is 2 to 1005. This argument identifies the TRBRF to which a TRCRF belongs and is required when defining a TRCRF.
mode {**srt** | **srb**}	(Optional) Specfifies the TRCRF bridging mode.
stp {**ieee** | **ibm** | **auto**}	(Optional) Specifies the Spanning Tree Protocol version for a TRBRF to use: source-routing transparent (**ieee**), source-route bridging (**ibm**), or automatic source selection (**auto**).

translation *vlan-number*	(Optional) Specifies a translational VLAN used to translate FDDI to Ethernet. Valid values are from 1 to 1005. This argument is not valid for defining or configuring Token Ring VLANs.
backupcrf {**off** | **on**}	(Optional) Specifies whether the TRCRF is a backup path for traffic.
aremaxhop *hop-count*	(Optional) Specifies the maximum number of hops for All-Routes Explorer frames. Possible values are 1 to 14. The default is 7. This argument is only valid when defining or configuring TRCRFs.
stemaxhop *hop-count*	(Optional) Specifies the maximum number of hops for Spanning-Tree Explorer frames. Possible values are 1 to 14. The default is 7. This argument is only valid when defining or configuring TRCRFs.

Defaults

The default configuration has all switched Ethernet ports and Ethernet repeater ports in VLAN 1. The default SAID is 100001 for VLAN 1, 100002 for VLAN 2, 100003 for VLAN 3, and so on. The default type is Ethernet. The default MTU is 1500 bytes. The default state is active.

The default TRBRF is 1005, the default TRCRF is 1003, and the default MTU for TRBRFs and TRCRFs is 4472. The default state is active. The default **aremaxhop** is 7; the default **stemaxhop** is 7.

Command Modes

Privileged EXEC

Usage Guidelines

You cannot use the **set vlan** command until the networking device is either in VTP transparent mode (**set vtp mode**) or until a VTP domain name has been set (**set vtp**).

Valid MTU values for Token Ring VLAN are 1500 or 4472. While you can enter any value for the MTU value, the value you enter defaults to the next lowest valid value.

You cannot set multiple VLANs for Inter-Switch Link (ISL) ports using this command. The VLAN name can be from 1 to 32 characters in length. If adding a new VLAN, the VLAN number must be within the range 2 to 1001. When modifying a VLAN, the valid range for the VLAN number is 2 to 1005.

On a new Token Ring VLAN, if you do not specify the parent parameter for a TRCRF, the default TRBRF (1005) is used.

Examples

The following example shows how to set VLAN 850 to include ports 4 through 7 on module 3. Because ports 4 through 7 were originally assigned to TRCRF 1003, the message reflects the modification of VLAN 1003.

```
Router# set vlan 850 3/4-7
VLAN 850 modified.
VLAN 1003 modified.
VLAN  Mod/Ports
---- ----------------------
850   3/4-7
```

Related Commands

Command	Description
clear vlan	Deletes an existing VLAN from a management domain.
show vlans	Displays VLAN subinterfaces.

set vlan mapping

To map 802.1Q virtual LANs (VLANs) to Inter-Switch Link (ISL) VLANs, use the **set vlan mapping** command in privileged EXEC mode.

set vlan mapping dot1q *1q-vlan-number* **isl** *isl-vlan-number*

Syntax Description

dot1q	Specifies the 802.1Q VLAN.
1q-vlan-number	Number identifying the 802.1Q VLAN; valid values are 1001 to 4095.
isl	Specifies the ISL VLAN.
isl-vlan-number	Number identifying the ISL VLAN; valid values are 1 to 1000.

Defaults

No 802.1Q-to-ISL mappings are defined.

Command Modes

Privileged EXEC

Usage Guidelines

IEEE 802.1Q VLAN trunks support VLANs 1 through 4095. ISL VLAN trunks support VLANs 1 through 1000. The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number.

The native VLAN of the 802.1Q trunk cannot be used in the mapping.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs. Note that if you map a 802.1Q VLAN over 1000 to an ISL VLAN, the corresponding 802.1Q VLAN will be blocked. For example, if you map 802.1Q VLAN 2000 to ISL VLAN 200, then 802.1Q VLAN 200 will be blocked.

You can map up to seven VLANs. Only one 802.1Q VLAN can be mapped to an ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

You cannot overwrite existing 802.1Q VLAN mapping. If the 802.1Q VLAN number is in the mapping table, the command is aborted. You must first clear that mapping.

If *vlan-number* does not exist, then either of the following occurs:

- If the switch is in server or transparent mode, the VLAN is created with all default values.
- If the switch is in client mode, then the command proceeds without creating the VLAN. A warning will be given indicating that the VLAN does not exist.

If the table is full, the command is aborted with an error message indicating the table is full.

Examples

The following example shows how to map VLAN 1022 to ISL VLAN 850:

```
Router# set vlan mapping dot1q 1022 isl 850
Vlan 850 configuration successful
Vlan mapping successful
```

The following example shows the display if you enter a VLAN that does not exist:

```
Router# set vlan mapping dot1q 1017 isl 999
```

```
Vlan mapping successful
Warning: vlan 999 non-existent
Vlan 999 configuration successful
```

The following example shows the display if you enter an existing mapping:

```
Router# set vlan mapping dot1q 1033 isl 722
722 exists in the mapping table. Please clear the mapping first.
```

The following example shows the display if the mapping table is full:

```
Router# set vlan mapping dot1q 1099 isl 917
Vlan Mapping Table Full.
```

Related Commands

Command	Description
clear vlan mapping	Deletes existing 802.1Q VLAN to ISL VLAN-mapped pairs.
show vlans	Displays VLAN subinterfaces.

shortcut-frame-count

To specify the maximum number of times a packet can be routed to the default router within shortcut-frame time before an MPOA resolution request is sent, use the **shortcut-frame-count** command in MPC configuration mode. To restore the default shortcut-setup frame count value, use the **no** form of this command.

shortcut-frame-count *count*

no shortcut-frame-count

Syntax Description

count	Shortcut-setup frame count. The default is 10 frames.

Defaults

The default is 10 frames.

Command Modes

MPC configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Examples

The following example sets the shortcut-setup frame count to 5 for the MPC:

```
shortcut-frame-count 5
```

Related Commands

Command	Description
atm-address	Overrides the control ATM address of an MPC or MPS.
mpoa client config name	Defines an MPC with a specified name.
shortcut-frame-time	Sets the shortcut-setup frame time (in seconds) for the MPC.

shortcut-frame-time

To set the shortcut-setup frame time (in seconds) for the MPC, use the **shortcut-frame-time** command in MPC configuration mode. To restore the default shortcut-setup frame-time value, use the **no** form of this command.

shortcut-frame-time *time*

no shortcut-frame-time

Syntax Description

time	Shortcut-setup frame time (in seconds).

Defaults

The default is 1 second.

Command Modes

MPC configuration

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Examples

The following example sets the shortcut-setup frame time to 7 for the MPC:

```
shortcut-frame-time 7
```

Related Commands

Command	Description
atm-address	Overrides the control ATM address of an MPC or MPS.
mpoa client config name	Defines an MPC with a specified name.
shortcut-frame-count	Specifies the maximum number of times a packet can be routed to the default router within shortcut-frame time before an MPOA resolution request is sent.

show adjacency

To display Cisco Express Forwarding (CEF) adjacency table information, use the **show adjacency** command in EXEC mode.

show adjacency [*type number*] [**detail**] [**summary**]

Syntax Description

type number	(Optional) Displays CEF adjacency information for the specified interface type and number.
detail	(Optional) Displays detailed adjacency information, including Layer 2 information.
summary	(Optional) Displays CEF adjacency table summary information.

Command Modes

EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.

Usage Guidelines

This command is used to verify that an adjacency exits for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.

Examples

The following is sample output from the **show adjacency detail** command:

```
Router# show adjacency detail

Protocol Interface                 Address
IP       Ethernet1/0/0             9.2.61.1(7)
                                   0 packets, 0 bytes
                                   00107BC30D5C
                                   00500B32D8200800
                                   ARP        02:01:49
```

The encapsulatuion string 00107BC30D5C00500B32D8200800 is that of an adjacency used for traffic switched out of a router on an Ethernet link using Ethernet II encapsulation.

The following is sample output from the **show adjacency summary** command:

```
Router# show adjacency summary

Adjacency Table has 1 adjacency
  Interface                Adjacency Count
  Ethernet1/0/0            1
```

Table 3 describes the significant fields shown in the displays.

Table 3 show adjacency detail Field Descriptions

Field	Description
Protocol	The routed protocol to which the adjacency is related.
Interface	The outgoing interface associated with the adjacency.
Address	The address can represent one of these addresses: • Next Hop address • Point-to-Point address The number (in parenthesis) that follows this field indicates the number of internal references to the adjacency.
Source	The source where the adjacency was learned.
Encapsulation string	The string which is prepended to a packet before the packet is transmitted.
Time stamp	The time left before the adjacency rolls out of the adjacency table. A packet must use the same next hop to the destination.

Related Commands

Command	Description
clear adjacency	Clears CEF adjacency table.

show atm vc

To display information about private ATM virtual circuits (VCs), use the following **show atm vc** privileged EXEC command.

show atm vc [*vcd*]

Syntax Description

vcd	(Optional) Specifies the VC to display information about.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

VCs on the extended MPLS ATM interfaces do not appear in the **show atm vc** command output. Instead, the **show xtagatm vc** command provides similar output that shows information only on extended MPLS ATM VCs.

Private VCs exist on the control interface of an MPLS Label Switch Controller (LSC) to support corresponding VCs on an extended MPLS ATM interface.

Examples

In the following example, 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 4 describes the significant fields shown in the output.

Table 4 show atm vc Field Descriptions

Field	Description
ATM1/0	Interface slot and number.
VCD	Virtual circuit descriptor (virtual circuit number).
VPI	Virtual path identifier.
VCI	Virtual circuit identifier.
etype	Ethernet type.
AAL5 - XTAGATM	Type of ATM adaptation layer (AAL) and encapsulation. A private VC has AAL5 and encapsulation XTAGATM.
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
PeakRate	Number of packets sent at the peak rate.
Average Rate	Number of packets sent at the average rate.
Burst Cells	Value that, when multiplied by 32, equals the maximum number of ATM cells the VC can send at the peak rate of the VC.

Table 4 show atm vc Field Descriptions (continued)

Field	Description
VCmode	AIP-specific or NPM-specific register describing the usage of the VC. Contains values such as rate queue, peak rate, and AAL mode, which are also displayed in other fields.
XTagATM1	Interface of corresponding extended MPLS ATM VC.
VCD	Virtual circuit descriptor (virtual circuit number) of the corresponding extended MPLS ATM VC.
VPI	Virtual path identifier of the corresponding extended MPLS ATM VC.
VCI	Virtual channel identifier of the corresponding extended MPLS ATM VC.
OAM frequency	Seconds between OAM loopback messages or DISABLED if OAM is not in use on this VC.
InARP frequency	Minutes between InARP messages, or DISABLED if InARP is not in use on this VC.
InPkts	Total number of packets received on this VC. This number includes all silicon-switched, fast-switched, autonomous-switched, and process-switched packets.
OutPkts	Total number of packets sent on this VC. This number includes all silicon-switched, fast-switched, autonomous-switched, and process-switched packets.
InBytes	Total number of bytes received on this VC. This number includes all silicon-switched, fast-switched, autonomous-switched, and process-switched packets.
OutBytes	Total number of bytes sent on this VC. This number includes all silicon-switched, fast-switched, autonomous-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.
OutFast	Number of fast-switched output packets.
InAS	Number of autonomous-switched or silicon-switched input packets.
OutAS	Number of autonomous-switched or silicon-switched output packets.
OAM F5 cells sent	Number of OAM cells sent on this VC.
OAM cells received	Number of OAM cells received on this VC.
Status	Displays the current state of the specified ATM interface.

show cable bundle

To display the forwarding table for the specified interface, use the **show cable bundle** privileged EXEC command.

show cable bundle *bundle-number forwarding-table*

Syntax Description

bundle-number	Specifies the bundle identifier. Valid range is from 1 to 255.
forwarding-table	Displays the forwarding table for the specified interface.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.

Examples

In the following example, a cable bundle of 25 is specified:

```
Router# show cable bundle 25 forwarding-table

MAC address         Interface
0050.7366.17ab      Cable3/0
0050.7366.1803      Cable3/0
0050.7366.1801      Cable3/0
```

The fields in the display are described as follows:

- MAC address—Media Access Control ID for each interface in the bundle.
- Interface—The cable interface slot and port number.

Related Commands

Command	Description
cable bundle	Creates an interface bundle.

show cef drop

To display a list of which packets each line card dropped, use the **show cef drop** command in user EXEC or privileged EXEC mode.

show cef drop

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(22)S	The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEF for IPv6 (dCEFv6) packets.
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. Previously there was a **show cef** command, and **drop** was a keyword of that command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

A line card might drop packets because of encapsulation failure, absence of route information, or absence of adjacency information.

A packet is sent to a different switching path (punted) because CEF does not support the encapsulation or feature, the packet is destined for the router, or the packet has IP options, such as time stamp and record route. IP options are process switched.

Note If CEFv6 or dCEFv6 is enabled globally on the router, the **show cef drop** command displays IPv6 CEF counter information and IPv4 CEF counter information. If CEFv6 or dCEFv6 is not enabled globally on the router, the command displays only IPv4 CEF counter information.

Examples

The following is sample output from the **show cef drop** command:

```
Router# show cef drop

CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj   ChksumErr
RP             4          89           0           4           0           0
1              0           0           0           0           0           0
2              0           0           5           0           0           5
IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj
RP             2          33           0           2           0
1              0           0           3           0           0
2              0           0           0           0           0
```

Table 5 describes the significant fields shown in the display.

Table 5 show cef drop Field Descriptions

Field	Description
Slot	The slot number on which the packets were received.
Encap_fail	Indicates the number of packets dropped after exceeding the limit for packets punted to the processor due to missing adjacency information (CEF throttles packets passed up to the process level at a rate of one packet per second).
Unresolved	Indicates the number of packets dropped due to an unresolved prefix in the Forwarding Information Base (FIB) table.
Unsupported	Indicates the number of packets fast-dropped by CEF (drop adjacency).
No_route	Indicates the number of packets dropped due to a missing prefix in the FIB table.
No_adj	Indicates the number of packets dropped due to incomplete adjacency.
ChksumErr	Indicates the number of IPv4 packets received with a checksum error. **Note** This field is not supported for IPv6 packets.

Related Commands

Command	Description
show cef interface	Displays CEF-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show cef events

To display a list of events internal to the CEF process, use the **show cef events** command in user EXEC or privileged EXEC mode.

show cef events

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

The following is sample output from the **show cef events** command:

```
Router# show cef events

CEF events (14/0 recorded/ignored)

Time            Event     Details
+00:00:00.000   SubSys    ipfib init
+00:00:00.000   SubSys    ipfib_ios init
+00:00:00.000   SubSys    ipfib_util init
+00:00:00.000   SubSys    adj_ios init
+00:00:00.000   SubSys    ipfib_les init
+00:00:01.272   Flag      FIB enabled set to yes
+00:00:01.272   Flag      FIB switching enabled set to yes
+00:00:01.272   GState    CEF enabled
+00:00:02.872   Process   Background created
+00:00:02.872   Flag      FIB running set to yes
+00:00:02.872   Process   Background event loop enter
+00:00:02.912   Flag      FIB switching running set to yes
+00:00:02.920   Process   Scanner created
+00:00:02.920   Process   Scanner event loop enter
```

Table 6 describes the significant fields shown in the display.

Table 6 show cef events Field Descriptions

Field	Description
Time	Time that the event occurred.
Event	Type of event that occurred.
Details	Detailed description of the event.

Related Commands

Command	Description
show cef drop	Displays a list of which packets each line card dropped.
show cef interface	Displays CEF-related interface information.
show cef linecard	Displays CEF-related interface information by line card.

show cef interface

To display detailed Cisco Express Forwarding (CEF) information for all interfaces, use the **show cef interface** command in EXEC mode.

show cef interface [*type number*] [**statistics**] [**detail**]

Syntax Description

type number	(Optional) Displays CEF information for the specified interface type and number.
statistics	(Optional) Displays switching statistics for the line card.
detail	(Optional) Displays detailed CEF information for the specified interface type and number.

Command Modes

EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(14)ST	Updated documentation for **statistics** keyword.
12.2(2)T	Updated documentation for **statistics** and **detail** keywords.

Usage Guidelines

You can use this command to show the detailed CEF status for all of the interfaces.

The *type number* arguments display CEF status information for the specified interface type and number.

Examples

The following is sample output from the **show cef interface detail** command for Ethernet interface 1/0/0:

```
Router# show cef interface Ethernet 1/0/0 detail

Ethernet1/0/0 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  Internet address is 9.2.61.8/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is Ethernet1/0/0
  Fast switching type 1, interface type 5
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
```

```
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A82 (0x48001A82)
  IP MTU 1500
```

The following is sample output from the **show cef interface Null 0 detail** command:

```
Router# show cef interface Null 0 detail

Null0 is up (if_number 1)
  Corresponding hwidb fast_if_number 1
  Corresponding hwidb firstsw->if_number 1
  Internet Protocol processing disabled
  Interface is marked as nullidb
  Packets switched to this interface on linecard are dropped to next slow path
  Hardware idb is Null0
  Fast switching type 13, interface type 0
  IP CEF switching enabled
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 0(0)
  Slot -1 Slot unit -1 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 1500
```

Table 7 describes the significant fields shown in the display.

Table 7 show cef interface Field Descriptions

Field	Description
Ethernet1/0/0 is {up | down}	Indicates type, number, and status of the interface.
Internet address is	Internet address of the interface.
ICMP redirects are always sent	Indicates how packet forwarding is configured.
Per packet load-sharing is disabled	Indicates status of load sharing on the interface.
IP unicast RPF check is disabled	Indicates status of IP unicast Reverse Path Forwarding (RPF) check on the interface.
Inbound access list is not set	Indicates the number or name of the inbound access list if one is applied to this interface.
Outbound access list is not set	Indicates the number or name of the outbound access list if one is applied to this interface.
IP policy routing is disabled	Indicates the status of IP policy routing on the interface.
Hardware idb is Ethernet1/0/0	Interface type and number configured.
Fast switching type	Used for troubleshooting; indicates switching mode in use.
interface type 5	Indicates interface type.
IP Distributed CEF switching enabled	Indicates whether distributed CEF is enabled on this interface. (7500 and 12000 series Internet routers only.)
IP Feature Fast switching turbo vector	Indicates IP fast switching type configured.
IP Feature CEF switching turbo vector	Indicates IP feature CEF switching type configured.

Table 7 show cef interface Field Descriptions (continued)

Field	Description
Input fast flags	Indicates the input status of various switching features as follows: • 0x0001 (input Access Control List [ACL] enabled) • 0x0002 (policy routing enabled) • 0x0004 (input rate limiting) • 0x0008 (MAC/Prec accounting) • 0x0010 (DSCP/PREC/QOS GROUP) • 0x0020 (input named access lists) • 0x0040 (NAT enabled on input) • 0x0080 (crypto map on input) • 0x0100 (QPPB classification) • 0x0200 (inspect on input) • 0x0400 (input classification) • 0x0800 (casa input enable) • 0x1000 (Virtual Private Network [VPN] enabled on a swidb) • 0x2000 (input idle timer enabled) • 0x4000 (unicast Reverse Path Forwarding [RPF] check) • 0x8000 (per-address ACL enabled) • 0x10000 (Deaggregating a packet) • 0x20000 (GPRS enabled on input) • 0x40000 (URL RenDezvous) • 0x80000 (QoS classification) • 0x100000 (FR switching on i/f) • 0x200000 (WCCP redirect on input) • 0x400000 (input classification)

Table 7 show cef interface Field Descriptions (continued)

Field	Description
Output fast flags	Indicates the output status of various switching features: • 0x0001 (output ACL enabled) • 0x0002 (IP accounting enabled) • 0x0004 (WCC redirect enable i/f) • 0x0008 (rate limiting) • 0x0010 (MAC/Prec accounting) • 0x0020 (DSCP/PREC/QOS GROUP) • 0x0040 (D-QOS classification) • 0x0080 (output named access lists) • 0x0100 (NAT enabled on output) • 0x0200 (TCP intercept enabled) • 0x0400 (crypto map set on output) • 0x0800 (output firewall) • 0x1000 (RSVP classification) • 0x2000 (inspect on output) • 0x4000 (QoS classification) • 0x8000 (QoS pre-classification) • 0x10000 (output stile)
ifindex 7/(7)	Indicates the SNMP ifindex for this interface.
Slot 1 Slot unit 0 VC -1	The slot number and slot unit.
Transmit limit accumulator	Indicates the maximum number of packets allowed in the transmit queue.
IP MTU	The value of the MTU size set on the interface.

Related Commands

Command	Description
show cef drop	Displays a list of which packets each line card dropped.
show cef linecard	Displays CEF-related interface information by line card.

show cef interface policy-statistics

To display detailed Cisco Express Forwarding (CEF) policy statistical information for all interfaces, use the **show cef interface policy-statistics** command in EXEC mode.

show cef interface [*type number*] **policy-statistics**

Syntax Description

type number	(Optional) Displays CEF information for the specified interface type and number.

Command Modes

EXEC

Command History

Release	Modification
12.0(9)S	This command was introduced to support the Cisco 12000 series Internet router.
12.0(14)ST	This command was introduced to support the Cisco 12000 series Internet router.

Usage Guidelines

This command is available only on distributed switching platforms.

The *type number* argument display CEF status information for the specified interface type and number.

Examples

The following is sample output from the **show cef interface policy-statistics** command:

```
Router# show cef interface ethernet 1/0 policy-statistics

Ethernet1/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
 Index         Packets            Bytes
     1               0                0
     2               0                0
     3               0                0
     4               0                0
     5               0                0
     6               0                0
     7               0                0
     8               0                0
```

Table 8 describes the significant fields shown in the output.

Table 8 show cef interface policy-statistics Field Descriptions

Field	Description
Index	Traffic index set with the **route-map** command.
Packts	Number of packets switched matching the index definition.
Bytes	Number of bytes switched matching the index definition.

Related Commands

Command	Description
show cef drop	Displays a list of which packets each line card dropped.
show cef linecard	Displays CEF-related interface information by line card.

show cef linecard

To display Cisco Express Forwarding (CEF)-related information by line card, use the **show cef linecard** command in EXEC mode.

show cef linecard [*slot-number*] [**detail**]

Syntax Description

slot-number	(Optional) Slot number containing the line card about which to display CEF-related information. When you omit this argument, information about all line cards is displayed.
detail	(Optional) Displays detailed CEF information for the specified line card.

Command Modes

EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(10)S	Output display was changed.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command is available only on distributed switching platforms.

When you omit the *slot-number* argument, information about all line cards is displayed. When you omit the *slot-number* argument and include the **detail** keyword, detailed information is displayed for all line cards. When you omit all keywords and arguments, the **show cef linecard** command displays important information about all line cards in table format.

Examples

The following is sample output from the **show cef linecard detail** command for all line cards:

```
Router# show cef linecard detail

CEF linecard slot number 0, status up
 Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
 Send failed 0, Out Of Sequence 0, drops 0
 Linecard CEF reset 0, reloaded 1
 95 elements packed in 6 messages(3588 bytes) sent
 69 elements cleared
 linecard in sync after reloading
 0/0/0 xdr elements in LowQ/MediumQ/HighQ
 11/9/69 peak elements on LowQ/MediumQ/HighQ
 Input  packets 0, bytes 0
 Output packets 0, bytes 0, drops 0
 CEF Table statistics:
 Table name                Version Prefix-xdr Status
 Default-table                   7          4 Active, up, sync
CEF linecard slot number 1, status up
```

```
Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
Send failed 0, Out Of Sequence 0, drops 0
Linecard CEF reset 0, reloaded 1
95 elements packed in 6 messages(3588 bytes) sent
69 elements cleared
linecard in sync after reloading
0/0/0 xdr elements in LowQ/MediumQ/HighQ
11/9/69 peak elements on LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0
CEF Table statistics:
Table name                Version Prefix-xdr Status
Default-table                   7          4 Active, up, sync
```

The following is sample output from the **show cef linecard** command. The command displays information for all line cards in table format.

```
Router# show cef linecard

Slot    MsgSent    XDRSent  Window   LowQ   MedQ  HighQ Flags
0             6         95      24      0      0      0 up
1             6         95      24      0      0      0 up
VRF Default-table, version 8, 6 routes
Slot Version    CEF-XDR    I/Fs State    Flags
0          7          4       8 Active   up, sync
1          7          4      10 Active   up, sync
```

Table 9 describes the significant fields shown in the displays.

Table 9 show cef linecard Field Descriptions

Field	Description
Table name	Name of the CEF table.
Version	Number of forwarding information base (FIB) table version.
Prefix-xdr	Number of prefix XDRs processed.
Status	State of the CEF table.
Slot	Slot number of the line card.
MsgSent	Number of interprocess communication (IPC) messages sent.
XDRSent	IPC information elements (XDRs) packed into IPC messages sent from the RP to the line card.
Window	Size of the IPC window between the line card and RP.
LowQ/MedQ/HighQ	Number of XDR elements in the Low, Medium, and High priority queues.
Flags	Indicates the status of the line card. Possible states are the following: • upLine card is up. • syncLine card is in synchronization with the main FIB. • FIB is repopulated on the line card. • resetLine card FIB is reset. • reloadingLine card FIB is being reloaded. • disabledLine card is disabled.

Table 9 show cef linecard Field Descriptions (continued)

Field	Description
CEF-XDR	Number of CEF XDR messages processed.
I/Fs	Interface numbers.

Related Commands

Command	Description
show cef drop	Displays a list of which packets each line card dropped.
show cef interface	Displays CEF-related interface information.

show cef not-cef-switched

To display which packets were sent to a different switching path, use the **show cef not-cef-switched** command in user EXEC or privileged EXEC mode.

show cef not-cef-switched

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(22)S	The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEF for IPv6 (dCEFv6) packets.
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. Previously there was a **show cef** command, and **drop** was a keyword of that command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

If packets are not being cef switched and you want to determine why, enter the **show cef not-cef switched** command.

Note If CEFv6 or dCEFv6 is enabled globally on the router, the **show cef not-cef-switched** command displays IPv6 CEF counter information and IPv4 CEF counter information. If CEFv6 or dCEFv6 is not enabled globally on the router, the command displays only IPv4 CEF counter information.

Examples

The following is sample output from the **show cef not-cef switched** command:

```
Router# show cef not-cef-switched

CEF Packets passed on to next switching layer
Slot No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access    Frag
RP         0         0          0        0    91584        0        0       0
1          0         0          0        0        0        0        0       0
2          0         0          0        0        0        0        0       0
IPv6 CEF Packets passed on to next switching layer
Slot No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access    MTU
RP         0         0          0        0    92784        0        0       0
1          0         0          0        0        0        0        0       0
2          0         0          0        0        0        0        0       0
```

Table 10 describes the significant fields shown in the display.

Table 10 show cef not-cef-switched Field Descriptions

Field	Meaning
Slot	The slot number on which the packets were received.
No_adj	Indicates the number of packets sent to the processor due to incomplete adjacency.
No_encap	Indicates the number of packets sent to the processor for Address Resolution Protocol (ARP) resolution.
Unsupp'ted	Indicates the number of packets punted to the next switching level due to unsupported features.
Redirect	Records packets that are ultimately destined to the router, and packets destined to a tunnel endpoint on the router. If the decapsulated tunnel is IP, it is CEF switched; otherwise, packets are process switched.
Receive	Indicates the number of packets ultimately destined to the router, or packets destined to a tunnel endpoint on the router. If the decapsulated tunnel packet is IP, the packet is CEF switched. Otherwise, packets are process switched.
Options	Indicates the number of packets with options. Packets with IP options are handled only at the process level.
Access	Indicates the number of packets punted due to an access list failure.
Frag	Indicates the number of packets punted due to fragmentation failure. **Note** This field is not supported for IPv6 packets.
MTU	Indicates the number of packets punted due to maximum transmission unit (MTU) failure. **Note** This field is not supported for IPv4 packets.

Related Commands

Command	Description
show cef drop	Display a list of which packets each line card dropped.
show cef interface	Displays CEF-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show cef timers

To display the current state of the timers internal to the CEF process, use the **show cef timers** command in user EXEC or privileged EXEC mode.

show cef timers

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.

Examples

The following is sample output from the **show cef timers** command:

```
Router# show cef timers

CEF background process
     Expiration   Type
            0.208 (parent)
               0.208 adjacency update hwidb
               0.540 slow resolution
               1.208 ARP throttle

CEF FIB scanner process
     Expiration    Type
           44.852  (parent)
              44.852  checker scan-rib
```

Table 11 describes the significant fields shown in the display.

Table 11 show cef timers Field Descriptions

Field	Description
Expiration	Seconds in which the timers will expire.
Type	Identification of the timer.

Related Commands

Command	Description
show cef interface	Displays CEF-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show controllers vsi control-interface

To display information about an ATM interface configured with the **tag-control-protocol vsi** EXEC command to control an external switch (or if an interface is not specified, to display information about all VSI control interfaces), use the **show controllers vsi control-interface** command.

show controllers vsi control-interface [*interface*]

Syntax Description

interface	(Optional) Specifies the interface number.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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.

Related Commands

Command	Description
tag-control-protocol vsi	Configures the use of VSI on a control port.

show controllers vsi descriptor

To display information about a switch interface discovered by the MPLS LSC through VSI, or if no descriptor is specified, about all such discovered interfaces, use the **show controllers vsi descriptor** EXEC command.

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*

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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** 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 12 describes the significant fields in the output.

Table 12 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 VPI 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

To display information about all sessions with VSI slaves, use the **show controllers vsi session** EXEC command.

show controllers vsi session [*session-num* [**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-num	(Optional) Specifies the session number.
interface *interface*	(Optional) Specifies the VSI control interface.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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 13 describes the significant fields in the output.

Table 13 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 14 describes the significant fields in the output.

Table 14 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 resent. 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.

Table 14 show controllers vsi session Field Descriptions (continued)

Field	Description
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.
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

To display a one-line summary of each VSI-controlled interface, use the **show controllers vsi status** EXEC command.

show controllers vsi status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Related Commands

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If an interface has been discovered by the LSC, but no extended MPLS ATM interface has been associated with it through the **extended-port** interface configuration 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 15 describes the significant fields in the output.

Table 15 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 15 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

To display traffic information about VSI-controlled interfaces, VSI sessions, or VCs on VSI-controlled interfaces, use the **show controllers vsi traffic** EXEC command.

show controllers vsi traffic [{**descriptor** *descriptor* | **session** *session-num* | **vc** [**descriptor** *descriptor* [*vpi vci*]]}]

Syntax Description

descriptor *descriptor*	(Optional) Specifies the interface.
session *session-num*	(Optional) Specifies a session number.
vc	(Optional) Virtual circuit.
vpi	(Optional) Virtual path identifier.
vci	(Optional) Virtual circuit identifier.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If none of the optional command parameters is specified, traffic for all interfaces is displayed. You can specify a single interface by its (switch-supplied) physical descriptor. For the BPX, the physical descriptor has the form *slot.port. 0*.

If a session number is specified, VSI protocol traffic counts by message type are displayed. The VC traffic display is the same as the one produced by the **show xtagatm vc cross-connect traffic descriptor** EXEC 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 16 describes the significant fields in the output.

Table 16 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 sent 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 sent on the interface due to traffic management and that 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 17 describes the significant fields in the output.

Table 17 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.

Table 17 show controllers vsi traffic session Field Descriptions (continued)

Field	Description
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.
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 that 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

To display information about an extended MPLS ATM interface controlled through the 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** EXEC command.

show controllers XTagATM *if-num*

Syntax Description

if-num	Specifies the interface number.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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** EXEC 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 18 describes the significant fields in the output.

Table 18 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.
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.”

Table 18 show controllers XTagATM Field Descriptions (continued)

Field	Description
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 stats

To display numbers of packets that were process switched, fast switched, and distributed switched, use the **show interface stats** command in EXEC mode.

show interface *type number* **stats**

Syntax Description

type number	Interface type and number about which to display statistics.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command on the RP.

Note When fast switching is configured on the outbound interface, and RSP optimum, RSP flow, and VIP DFS switching modes are all specified on the incoming interface, the interface on which RSP optimum, RSP flow, and VIP DFS switching modes is not enabled can still show packets switched out via those switching paths when packets are received from other interfaces with RSP optimum, RSP flow, and VIP DES switching modes enabled.

Examples

The following is sample output from the **show interface stats** command:

```
Router# show interface fddi 3/0/0 stats

Fddi3/0/0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor    3459994 1770812197    4141096 1982257456
             Route cache   10372326 3693920448     439872  103743545
       Distributed cache   19257912 1286172104   86887377 1184358085
                   Total   33090232 2455937453   91468345 3270359086
```

Table 19 describes the significant fields in the display.

Table 19 show interface stats Field Descriptions

Field	Description
Fddi3/0/0	Interface for which information is shown.
Switching path	Column heading for the various switching paths below it.
Pkts In	Number of packets received in each switching mechanism.
Chars In	Number of characters received in each switching mechanism.

Table 19 show interface stats Field Descriptions (continued)

Field	Description
Pkts Out	Number of packets sent out each switching mechanism.
Chars Out	Number of characters sent out each switching mechanism.

show interface XTagATM

To display information about an extended MPLS ATM interface, use the **show interface XTagATM** EXEC command.

show interface XTagATM *if-num*

Syntax Description

if-num	Specifies the MPLS ATM interface number.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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 output from the **show interface XTagATM** command:

```
Router# show interface XTagATM0

XTagATM0 is up, line protocol is up
  Hardware is Tag-Controlled Switch Port
  Interface is unnumbered.  Using address of Loopback0 (12.0.0.17)
  MTU 4470 bytes, BW 156250 Kbit, DLY 80 usec, rely 255/255, load 1/255
  Encapsulation ATM Tagswitching, loopback not set
  Encapsulation(s): AAL5
  Control interface: ATM1/0, switch port: bpx 10.2
  9 terminating VCs, 16 switch cross-connects
  Switch port traffic:
     129302 cells input, 127559 cells output
  Last input 00:00:04, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Terminating traffic:
  5 minute input rate 1000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     61643 packets input, 4571695 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     53799 packets output, 4079127 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffers copied, 0 interrupts, 0 failures
```

Table 20 describes the significant fields in the sample command output shown above.

Table 20 show interface XTagATM Field Descriptions

Field	Description
XTagATM0 is up	Interface is currently active.
line protocol is up	Displays the line protocol as up.
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.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation ATM Tagswitching	Encapsulation method.
loopback not set	Indicates that loopback is not set.
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.
9 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.
16 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 counts	Indicates that counters below this line apply only to packets sent or received on terminating VCs.
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.

Table 20 show interface XTagATM Field Descriptions (continued)

Field	Description
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.
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.

Table 20 show interface XTagATM Field Descriptions (continued)

Field	Description
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.
output buffers copied	Number of packets copied from a MEMD buffer into a system buffer before being placed on the output hold queue.
interrupts	Displays the value of hwidb to tx_restarts.
failures	Number of packets discarded because no MEMD buffer was available.

Related Commands

Command	Description
interface XTagATM	Enters configuration mode for an extended MPLS ATM (XTagATM) interface.

show ip bgp vpnv4

To display VPN address information from the BGP table, use the **show ip bgp vpnv4** command in EXEC mode.

show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [*ip-prefix/length* [**longer-prefixes**] [*output-modifiers*]] [*network-address* [*mask*] [**longer-prefixes**] [*output-modifiers*]] [**cidr-only**] [**community**] [**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**][**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**tags**]

Syntax Description

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays NLRIs that have a matching route distinguisher.
vrf *vrf-name*	Displays NLRIs associated with the named VRF.
ip-prefix/length	(Optional) IP prefix address (in dotted decimal format) and length of mask (0 to 32).
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.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
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 nonnatural net masks.
community	(Optional) Displays routes matching this community.
community-list	(Optional) Displays routes matching this community list.
dampened-paths	(Optional) Displays paths suppressed on account of dampening (BGP route from peer is up and down).
filter-list	(Optional) Displays routes conforming 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 AS paths.
peer-group	(Optional) Displays information about peer groups.
quote-regexp	(Optional) Displays routes matching the AS path "regular expression."
regexp	(Optional) Displays routes matching the AS path regular expression.
summary	(Optional) Displays BGP neighbor status.
tags	(Optional) Displays incoming and outgoing BGP labels for each NLRI.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** EXEC command displays all available VPNv4 information. The **show ip bgp vpnv4 summary** EXEC command displays BGP neighbor status.

Examples

The following example shows output for all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 14.14.14.14
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: 100:1 (vrf1)
*> 11.0.0.0         50.0.0.1 0 0 101 i
*>i12.0.0.0         13.13.13.13 0    100 0 102 i
*> 50.0.0.0         50.0.0.1 0 0 101 i
*>i51.0.0.0         13.13.13.13 0    100 0 102 i
```

Table 21 describes the significant fields shown in the output.

Table 21 show ip bgp vpnv4 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 NLRIs that have a route-distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 tags

NetworkNext Hop      In tag/Out tag
Route Distinguisher: 100:1 (vrf1)
   2.0.0.0          10.20.0.60      34/notag
   10.0.0.0         10.20.0.60      35/notag
   12.0.0.0         10.20.0.60      26/notag
```

```
                  10.20.0.60      26/notag
   13.0.0.0       10.15.0.15      notag/26
```

Table 22 describes the significant fields shown in the output.

Table 22 show ip bgp vpnv4 rd tags Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In Tag	Displays the label (if any) assigned by this router.
Out Tag	Displays the label assigned by the BGP next hop router.

The following example shows VPNv4 routing entries for the VRF called vrf1.

```
Router# show ip bgp vpnv4 vrf vrf1

BGP table version is 18, local router ID is 14.14.14.14
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: 100:1 (vrf1)
*> 11.0.0.0         50.0.0.1 0 0 101 i
*>i12.0.0.0         13.13.13.13 0    100 0 102 i
*> 50.0.0.0         50.0.0.1 0 0 101 i
*>i51.0.0.0         13.13.13.13 0    100 0 102 i
```

Table 23 describes the significant fields shown in the output.

Table 23 show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays network address from the BGP table.
Next Hop	Displays 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.

Related Commands

Command	Description
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip cache

To display the routing table cache used to fast switch IP traffic, use the **show ip cache** EXEC command.

show ip cache [*prefix mask*] [*type number*]

Syntax Description

prefix	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
type	(Optional) Displays only the entries in the cache that match the interface type and number combination.
number	(Optional) Displays only the entries in the cache that match the interface type and number combination.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **show ip cache** display shows MAC headers up to 92 bytes.

Examples

The following is sample output from the **show ip cache** command:

```
Router# show ip cache

IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last 7 seconds, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago

Prefix/Length       Age       Interface       MAC Header
131.108.1.1/32      0:01:09   Ethernet0/0     AA000400013400000C0357430800
131.108.1.7/32      0:04:32   Ethernet0/0     00000C01281200000C0357430800
131.108.1.12/32     0:02:53   Ethernet0/0     00000C029FD000000C0357430800
131.108.2.13/32     0:06:22   Fddi2/0         00000C05A3E000000C035753AAAA0300
                                              00000800
131.108.2.160/32    0:06:12   Fddi2/0         00000C05A3E000000C035753AAAA0300
                                              00000800
131.108.3.0/24      0:00:21   Ethernet1/2     00000C026BC600000C03574D0800
131.108.4.0/24      0:02:00   Ethernet1/2     00000C026BC600000C03574D0800
131.108.5.0/24      0:00:00   Ethernet1/2     00000C04520800000C03574D0800
131.108.10.15/32    0:05:17   Ethernet0/2     00000C025FF500000C0357450800
131.108.11.7/32     0:04:08   Ethernet1/2     00000C010E3A00000C03574D0800
131.108.11.12/32    0:05:10   Ethernet0/0     00000C01281200000C0357430800
131.108.11.57/32    0:06:29   Ethernet0/0     00000C01281200000C0357430800
```

Table 24 describes the significant fields shown in the output.

Table 24 show ip cache Field Descriptions

Field	Description
IP routing cache version	Version number of this table. This number is incremented any time the table is flushed.
entries	Number of valid entries.
bytes	Number of bytes of processor memory for valid entries.
hash overflows	Number of times autonomous switching cache overflowed.
Minimum invalidation interval	Minimum time delay between cache invalidation request and actual invalidation.
maximum interval	Maximum time delay between cache invalidation request and actual invalidation.
quiet interval	Length of time between cache flush requests before the cache will be flushed.
threshold <*n*> requests	Maximum number of requests that can occur while the cache is considered quiet.
Invalidation rate <*n*> in last <*m*> seconds	Number of cache invalidations during the last <*m*> seconds.
0 in last 3 seconds	Number of cache invalidation requests during the last quiet interval.
Last full cache invalidation occurred <*hh:mm:ss*> ago	Time since last full cache invalidation was performed.
Prefix/Length	Network reachability information for cache entry.
Age	Age of cache entry.
Interface	Output interface type and number.
MAC Header	Layer 2 encapsulation information for cache entry.

The following is sample output from the **show ip cache** command with a prefix and mask specified:

```
Router# show ip cache 131.108.5.0 255.255.255.0

IP routing cache version 4490, 119 entries, 17464 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:11:56 ago

Prefix/Length       Age       Interface       MAC Header
131.108.5.0/24      0:00:34   Ethernet1/2     00000C04520800000C03574D0800
```

The following is sample output from the **show ip cache** command with an interface specified:

```
Router# show ip cache e0/2

IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago

Prefix/Length       Age       Interface       MAC Header
131.108.10.15/32    0:05:17   Ethernet0/2     00000C025FF500000C0357450800
```

show ip cache flow

To display a summary of the NetFlow switching statistics, use the **show ip cache flow** command in EXEC mode.

show ip cache [*prefix mask*] [*type number*] [**verbose**] **flow**

Syntax Description

prefix mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
type number	(Optional) Displays only the entries in the cache that match the interface type and number combination.
verbose	(Optional) Displays additional information

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
11.1 CA	The information display for the command was updated.

Usage Guidelines

Some of the content in the display of the **show ip cache flow** command uses multiline headings and multiline data fields. Figure 2 shows how to associate the headings with the correct data fields when there are two lines of headings and two lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields.

When other features are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same.

Figure 2 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the show ip cache flow Command

```
Router#show ip cache flow
IP packet size distribution (230151 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .999 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456448 bytes
  65509 active, 27 inactive, 820628747 added
  955454490 ager polls, 0 flow alloc failures
  Exporting flows to 1.1.15.1 (2057)
  820563238 flows exported in 34485239 udp datagrams, 0 failed

  last clearing of statistics 00:00:03

Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-BGP            71      0.0         1    49      0.0       2.5      15.8
UDP-other          17      0.0         1   328      0.0       0.0      15.7
ICMP            18966      6.7        10    28     72.9       0.1      22.9
Total:          19054      6.7        10    28     72.9       0.1      22.9

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et1/1          52.52.52.1      Fd4/0          42.42.42.1      01 55  10    3748
0000 /8  50                    0000 /8  40    202.120.130.2          28    17.8
Et1/2          52.52.52.1      Fd4/0          42.42.42.1      01 CC  10    3568
0000 /8  50                    0000 /8  40    202.120.130.2          28    17.8
Et1/2          10.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1124
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          11.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1157
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.7
```

127034

Displaying NetFlow Cache Information on a Distributed Cisco 7500 Series Platform

To display NetFlow cache information using the **show ip cache flow** command on a Cisco 7500 series router that is running dCEF, enter the following sequence of commands:

```
Router# if-con slot-number
LC-slot-number# show ip cache [prefix mask] [type number] [verbose] flow
```

Displaying NetFlow Cache Information on a Distributed Cisco 12000 Series Platform

To display NetFlow cache information using the **show ip cache flow** command on a Cisco 12000 Series Internet router, you enter the following sequence of commands:

```
Router# attach slot-number
LC-slot-number# show ip cache [prefix mask] [type number] [verbose] flow
```

Examples

The following is an example display of a main cache using the **show ip cache flow** command:

```
Router# show ip cache flow

IP packet size distribution (230151 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .999 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
```

```
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

The output above shows the percentage distribution of packets by size range. In this display, 99.9 percent of the packets fall in the size range from 1 to 32 bytes.

```
IP Flow Switching Cache, 4456448 bytes
  65509 active, 27 inactive, 820628747 added
  955454490 ager polls, 0 flow alloc failures
  Exporting flows to 1.1.15.1 (2057)
  820563238 flows exported in 34485239 udp datagrams, 0 failed
  last clearing of statistics 00:00:03

Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-BGP             71      0.0         1    49      0.0       2.5      15.8
UDP-other           17      0.0         1   328      0.0       0.0      15.7
ICMP             18966      6.7        10    28     72.9       0.1      22.9
Total:           19054      6.7        10    28     72.9       0.1      22.9

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et1/1          52.52.52.1      Fd4/0          42.42.42.1      01 55  10    3748
0000 /8  50                    0000 /8  40    202.120.130.2          28    17.8
Et1/2          52.52.52.1      Fd4/0          42.42.42.1      01 CC  10    3568
0000 /8  50                    0000 /8  40    202.120.130.2          28    17.8
Et1/2          10.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1124
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          11.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1157
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.7
Et1/2          14.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1149
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          15.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1127
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.7
Et1/2          12.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1204
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          13.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1159
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          18.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1223
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          19.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1264
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          16.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1170
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          17.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1167
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          22.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1193
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.8
Et1/2          23.1.3.2        Fd4/0          42.42.42.1      01 C0  10    1212
0000 /0  0                     0000 /8  40    202.120.130.2          28    17.7
Et1/1          50.50.50.1      Local          31.31.31.1      06 C0  18       2
00B3 /32 0                     2AF8 /32 0     0.0.0.0                49    10.1
```

The following shows sample output from the **show ip cache** *prefix mask* **flow** command:

```
Router# show ip cache 10.0.0.1 256.0.0.0 flow

IP packet size distribution (25 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

The output above shows the percentage distribution of packets by size range. In this display, 100 percent of the packets fall in the128 byte range.

```
IP Flow Switching Cache, 4456704 bytes
  1 active, 65535 inactive, 5 added
  68 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never

Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                 4      0.0         5   100      0.0       0.0      15.2
Total:               4      0.0         5   100      0.0       0.0      15.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et1/2         10.0.0.2        Local         10.0.0.1        01 0000 0800     5
```

The following shows sample output from the **show ip cache** *type number* **flow** command:

```
Router# show ip cache e1/2 flow

IP packet size distribution (30 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

IP Flow Switching Cache, 4456704 bytes
  1 active, 65535 inactive, 6 added
  85 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never

Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                 5      0.0         5   100      0.0       0.0      15.1
Total:               5      0.0         5   100      0.0       0.0      15.1

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et1/2         10.0.0.2        Local         10.0.0.1        01 0000 0800     5
```

Table 25 describes the significant fields shown in the flow switching cache lines of the display.

Table 25 show ip cache flow Field Descriptions in Flow Switching Cache Display

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire (used by Cisco for diagnostics only).

Table 25 show ip cache flow Field Descriptions in Flow Switching Cache Display (continued)

Field	Description
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Exporting flows	IP address and User Datagram Protocol (UDP) port number of the workstation to which flows are exported.
flows exported in udp datagrams	Total number of flows exported and the total number of UDP datagrams used to export the flows to the workstation.
failed	Number of flows that could not be exported by the router because of output interface limitations.
last clearing of statistics	Standard time output (hh:mm:ss) since the **clear ip flow stats** EXEC command was executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 26 describes the significant fields shown in the activity by protocol lines of the display.

Table 26 show ip cache flow Field Descriptions in Activity By Protocol Display

Field	Description
Protocol	IP protocol and the “well known” port number as described in RFC 1340.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol seen per second; equal to total flows/number of seconds for this summary period.
Packets/Flow	Average number of packets observed for the flows seen for this protocol. Equal to total packets for this protocol or number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of packet for this protocol for this summary period).
Packets/Sec	Average number of packets for this protocol per second (total packets for this protocol) or the total number of seconds for this summary period.
Active(Sec)/Flow	Sum of all the seconds from the first packet to the last packet of an expired flow (for example, TCP FIN, timeout, and so on) in seconds or total flows for this protocol for this summary period.
Idle(Sec)/Flow	Sum of all the seconds from the last packet seen in each nonexpired flow for this protocol until the time at which this command was entered, in seconds or total flows for this protocol for this summary period.

The following sample output is for the **show ip cache flow** command when the **tunnel flow egress-records** command enables a generic routing encapsulation (GRE) tunnel with both Cisco Express Forwarding (CEF) and NetFlow configured. The last line is a NetFlow record that is created for packets that are encapsulated by a tunnel.

```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se3/2         10.1.0.1        Tu0            40.1.1.1       01 0000 0800    5
Local         100.20.1.1      Fa0/0         100.20.1.2      2F 0000 0000    5
```

Table 27 describes the significant fields in the NetFlow record lines of the displays:

Table 27 show ip cache flow Field Descriptions in NetFlow Record Display

Field	Description
SrcIf	Interface on which the packet was received.
SrcIPaddress	IP address of the device which transmitted the packet.
DstIf	Interface from which the packet was transmitted.
DstIPaddress	IP address of the destination device.
Pr	IP protocol "well-known" port number as described in RFC 1340, displayed in hexadecimal format.
SrcP	IP port from which the packet is transmitted, displayed in hexadecimal format.
DstP	IP port where the packet is to be delivered, displayed in hexadecimal format.
Pkts	Number of packets switched through this flow.

The following shows sample output from the **show ip cache verbose flow** command for interface e1/2 on 10.0.0.1 255.0.0.0:

```
Router# show ip cache 10.0.0.1 255.0.0.0 e1/2 verbose flow

IP packet size distribution (35 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

The output above show the percentage distribution of packets by size range. In this display,100 percent of the packets fall in the 138 byte size range.

```
IP Flow Switching Cache, 4456704 bytes
  1 active, 65535 inactive, 7 added
  99 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never

Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                 6      0.0         5   100      0.0       0.0      15.2
Total:               6      0.0         5   100      0.0       0.0      15.2

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et1/2          10.0.0.2        Local          10.0.0.1        01 00  10       5
0000 /8  0                     0800 /8  0     0.0.0.0                100     0.0
```

Table 28 describes the significant fields in the NetFlow record lines of the display.

Table 28 show ip cache verbose flow Field Descriptions in NetFlow Record Display

Field	Description
SrcIf	Interface on which the packet was received.
Port Msk AS	Source Border Gateway Protocol (BGP) autonomous system. This is always set to 0 in MPLS flows.

Table 28 show ip cache verbose flow Field Descriptions in NetFlow Record Display (continued)

Field	Description
SrcIPaddress	IP address of the device which transmitted the packet.
DstIf	Interface from which the packet was transmitted.
Port Msk AS	Destination BGP autonomous system. This is always set to 0 in MPLS flows.
DstIPaddress	IP address of the destination device.
NextHop	Specifies the BGP next hop address. This is always set to 0 in MPLS flows.
Pr	IP protocol well-known port number as described in RFC 1340, displayed in hexadecimal format.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Flgs	TCP flags (result of bitwise OR of TCP flags from all packets in the flow).
Active	Number of active flows in the NetFlow cache at the time this command was entered.
Pkts	Number of packets switched through this flow.

Related Commands

Command	Description
clear ip flow stats	Clears the NetFlow switching statistics.
ip route-cache	Controls the use of high-speed switching caches for IP routing.
tunnel flow egress-records	Creates a NetFlow record for packets that are encapsulated by the GRE tunnel.

show ip cache flow aggregation

To display the aggregation cache configuration, use the **show ip cache flow aggregation** command in EXEC mode.

show ip cache [*prefix mask*] [*type number*] [**verbose**] **flow aggregation** *type*

Syntax Description

prefix mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
type number	(Optional) Displays only the entries in the cache that match the interface type and number combination.
verbose	(Optional) Displays additional information from the aggregation cache.
type	Displays the configuration of a particular aggregation cache as follows: • Autonomous system • Destination prefix • Prefix • Protocol-port • Source prefix

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

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

Examples

The following is an example display of an autonomous system aggregation cache using the **show ip cache flow aggregation as** command:

```
Router# show ip cache flow aggregation as

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If       Src AS  Dst If       Dst AS  Flows   Pkts  B/Pk  Active
Fa1/0         0      Null          0         1      2     49    10.2
Fa1/0         0      Se2/0         20        1      5    100     0.0
```

The following is a sample display of an autonomous system aggregation cache for the prefix mask 10.0.0.1 255.0.0.0 using the **show ip cache flow aggregation as** command:

```
Router# show ip cache 10.0.0.1 255.0.0.0 flow aggregation as

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If         Src AS  Dst If         Dst AS     Flows    Pkts  B/Pk  Active
e1/2            0      Null            0            1     2       49    10.2
e1/2            0      e1/2           20            1     5      100     0.0
```

The following is a sample display of an autonomous system aggregation cache for 10.0.0.1 255.0.0.0 Ethernet1/2 using the **show ip cache verbose flow aggregation as** command:

```
Router# show ip cache 10.0.0.1 255.0.0.0 e1/2 verbose flow aggregation as

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If         Src AS  Dst If         Dst AS     Flows    Pkts  B/Pk  Active
e1/2            0      Null            0            1     2       49    10.2
e1/2            0      e1/2           20            1     5      100     0.0
```

Table 29 describes the significant fields shown in these examples.

Table 29 show ip cache flow aggregation Field Descriptions

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Src If	Specifies the source interface.
Src AS	Specifies the source autonomous system.
Dst If	Specifies the destination interface.
Dst AS	Specifies the destination autonomous system.
Flows	Number of flows.
Pkts	Number of packets.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Active	Number of active flows in the NetFlow cache at the time this command was entered.

Related Commands

Command	Description
ip flow-aggregation cache	Enables aggregation cache configuration mode.

show ip cef

To display entries in the forwarding information base (FIB) or to display a summary of the FIB, use the **show ip cef** command in EXEC mode:

show ip cef [**vrf** *vrf-name*] [[**unresolved** [**detail**]] | [**detail** | **summary**]]

Specific FIB Entries Based on IP Address Information

show ip cef [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]

Specific FIB Entries Based on Interface Information

show ip cef [**vrf** *vrf-name*] [*type number*] [**detail**]

Specific FIB Entries Based on Nonrecursive Routes

show ip cef [**vrf** *vrf-name*] **non-recursive** [**detail**]

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
unresolved	(Optional) Displays unresolved FIB entries.
detail	(Optional) Displays detailed FIB entry information.
summary	(Optional) Displays a summary of the FIB.
network	(Optional) Displays the FIB entry for the specified destination network.
mask	(Optional) Displays the FIB entry for the specified destination network and mask.
longer-prefixes	(Optional) Displays FIB entries for more specific destinations.
type number	(Optional) Interface type and number for which to display FIB entries.
non-recursive	Displays only nonrecursive routes.

Command Modes

EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(5)T	The **vrf** keyword was added.

Usage Guidelines

The **show ip cef** command without any keywords or arguments shows a brief display of all FIB entries.

The **show ip cef detail** command shows detailed FIB entry information for all FIB entries.

Examples

The following is sample output from the **show ip cef unresolved** command:

```
Router# show ip cef unresolved

IP Distributed CEF with switching (Table Version 136632)
45776 routes, 13 unresolved routes (0 old, 13 new)
45776 leaves, 2868 nodes, 8441480 bytes, 136632 inserts, 90856 invalidations
1 load sharing elements, 208 bytes, 1 references
1 CEF resets, 1 revisions of existing leaves
refcounts: 527292 leaf, 465617 node

148.214.0.0/16, version 136622
0 packets, 0 bytes
  via 171.69.233.56, 0 dependencies, recursive
  unresolved
148.215.0.0/16, version 136623
0 packets, 0 bytes
  via 171.69.233.56, 0 dependencies, recursive
  unresolved
148.218.0.0/16, version 136624
0 packets, 0 bytes
```

Table 30 describes the significant fields shown in the display.

Table 30 show ip cef unresolved Field Descriptions

Field	Description
routes	Total number of entries in the CEF table
unresolved routes	Number of entries in the CEF table that do not have resolved recursions categorized by old and new routes
leaves, nodes, bytes	Number of elements in the CEF Trie and how much memory they use
inserts	Number of nodes inserted
invalidations	Number of entries that have been invalidated
load sharing elements, bytes, references	Information about load sharing elements: how many, number of associated bytes, and number of associated references
version	Version of the CEF table
packets, bytes	Number of packets and bytes switched through the name entry
dependencies	Number of table entries which point to the named entry
recursive	Indicates that the destination is reachable through another route
unresolved	Number of entries that do not have resolved recursions

The following is sample output from the **show ip cef summary** command:

```
Router# show ip cef summary

IP Distributed CEF with switching (Table Version 135165)
45788 routes, 0 reresolve, 4 unresolved routes (0 old, 4 new)
45788 leaves, 2868 nodes, 8442864 bytes, 135165 inserts, 89377 invalidations
0 load sharing elements, 0 bytes, 0 references
1 CEF resets, 0 revisions of existing leaves
refcounts: 527870 leaf, 466167 node
```

For a description of significant fields in this display, see Table 30.

The following is sample output from the **show ip cef detail** command for Ethernet interface 0. It shows all the prefixes resolving through adjacency pointing to next hop Ethernet interface 0/0 and next hop interface IP address 172.19.233.33.

```
Router# show ip cef e0/0 172.19.233.33 detail

IP Distributed CEF with switching (Table Version 136808)
45800 routes, 8 unresolved routes (0 old, 8 new) 45800 leaves, 2868 nodes, 8444360 bytes,
136808 inserts, 91008 invalidations 1 load sharing elements, 208 bytes, 1 references 1 CEF
resets, 1 revisions of existing leaves refcounts: 527343 leaf, 465638 node

172.19.233.33/32, version 7417, cached adjacency 172.19.233.33 0 packets, 0 bytes,
Adjacency-prefix
via 172.19.233.33, Ethernet0/0, 0 dependencies
next hop 172.19.233.33, Ethernet0/0
valid cached adjacency
```

Table 31 describes the significant fields in the display.

Table 31 show ip cef detail Field Descriptions

Field	Description
routes	Total number of entries in the CEF table
unresolved routes	Number of entries in the CEF table that do not have resolved recursions categorized by old and new routes
leaves, nodes, bytes	Number of elements in the CEF Trie and how much memory they use
inserts	Number of nodes inserted
invalidations	Number of entries that have been invalidated
load sharing elements, bytes, references	Information about load sharing elements: how many, number of associated bytes, and number of associated references
version	Version of the CEF table
cached adjacency	Type of adjacency to which this CEF table entry points
packets, bytes	Number of packets and bytes switched through the name entry
dependencies	Number of table entries which point to the named entry
next hop	Type of adjacency or the next hop toward the destination

The following example shows the forwarding table associated with the VRF named vrf1:

```
Router# show ip cef vrf vrf1

Prefix              Next Hop            Interface
0.0.0.0/32          receive
11.0.0.0/8          50.0.0.1            Ethernet1/3
12.0.0.0/8          52.0.0.2            POS6/0
50.0.0.0/8          attached            Ethernet1/3
50.0.0.0/32         receive
50.0.0.1/32         50.0.0.1            Ethernet1/3
50.0.0.2/32         receive
50.255.255.255/32   receive
51.0.0.0/8          52.0.0.2            POS6/0
224.0.0.0/24        receive
255.255.255.255/32  receive
```

Table 32 describes the significant fields shown in the display.

Table 32 show ip cef vrf Field Descriptions

Field	Description
Prefix	Specifies the network prefix.
Next Hop	Specifies the Border Gateway Protocol (BGP) next hop address.
Interface	Specifies the VRF interface.

Related Commands

Command	Description
show cef drop	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show cef interface	Displays CEF-related interface information.

show ip cef adjacency

To display Cisco Express Forwarding (CEF) recursive and direct prefixes resolved through an adjacency, use the **show ip cef adjacency** command in EXEC mode.

show ip cef [**vrf** *vrf-name*] **adjacency** *type number ip-prefix* [**detail**]

To display CEF recursive and direct prefixes resolved through special adjacency types representing nonstandard switching paths, use this form of the **show ip cef adjacency** EXEC command.

show ip cef [**vrf** *vrf-name*] **adjacency** {**discard** | **drop** | **glean** | **null** | **punt**} [**detail**]

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
type number	Interface type and number for which to display forwarding information base (FIB) entries.
ip-prefix	Next hop IP prefix, in dotted decimal format (A.B.C.D).
detail	(Optional) Displays detailed information for each CEF adjacency type entry.
discard	Discard adjacency. Sets up for loopback interfaces. Loopback IP addresses are receive entries in the FIB table.
drop	Drop adjacency. Packets forwarded to this adjacency are dropped.
glean	Glean adjacency. Represents destinations on a connected interface for which no ARP cache entry exists.
null	Null adjacency. Formed for the Null0 interface. Packets forwarded to this adjacency are dropped.
punt	Punt adjacency. Represents destinations that cannot be switched in the normal path and that are punted to the next fastest switching vector.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.
12.0(5)T	The **vrf** keyword was added.

Usage Guidelines

An adjacency is a node that can be reached by one Layer 2 hop.

This command shows all prefixes resolved through a regular next hop adjacency or through a special adjacency type such as discard, drop, glean, null and punt.

The following sample output is from the **show ip cef adjacency** command when the **glean** type is specified.

```
Router# show ip cef adjacency glean

Prefix              Next Hop            Interface
```

```
9.2.61.0/24         attached            Ethernet1/0/0
172.17.250.252/32   9.2.61.1            Ethernet1/0/0
```

The following sample output is from the **show ip cef adjacency drop** command with **detail** specified:

```
Router# show ip cef adjacency drop detail

IP CEF with switching (Table Version 4), flags=0x0
  4 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 0
  4 leaves, 8 nodes, 8832 bytes, 13 inserts, 9 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id 00B999CA
  3 CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place modifications
  refcounts:  533 leaf, 536 node

224.0.0.0/4, version 3
0 packets, 0 bytes, Precedence routine (0)
  via 0.0.0.0, 0 dependencies
    next hop 0.0.0.0
    valid drop adjacency
```

The following sample output shows the direct IP prefix when the next hop Gigabit Ethernet interface 3/0 is specified:

```
Router# show ip cef adjacency GigabitEthernet 3/0 172.20.26.29

Prefix              Next Hop            Interface
34.1.1.0/24         172.20.26.29        GigabitEthernet3/0
```

Table 33 describes the significant fields shown in the display.

Table 33 show ip cef adjacency Field Descriptions

Field	Description
Prefix	Destination IP prefix.
Next Hop	Next hop IP address.
Interface	Next hop interface.

Related Commands

Command	Description
show adjacency	Displays CEF adjacency table information.

show ip cef events

To display all recorded Cisco Express Forwarding (CEF) forwarding information base (FIB) and adjacency events, use the **show ip cef events** command in EXEC mode.

show ip cef [**vrf** *vrf-name*] **events** [*ip-prefix*] [**new** | **within** *seconds*] [**detail**] [**summary**]

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
ip-prefix	(Optional) Next hop IP prefix, in dotted decimal format (A.B.C.D).
new	(Optional) Displays new CEF events not previously shown.
within *seconds*	(Optional) Displays CEF events that occurred within a specified number of seconds.
detail	(Optional) Displays detailed information for each CEF event entry.
summary	(Optional) Displays a summary of the CEF event log.

Command Modes

EXEC

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command shows the state of the table event log and must be enabled for events to record.

The **ip cef table event-log** command controls parameters such as event log size.

Examples

The following sample output is from the **show ip cef events** command with **summary** specified:

```
Router# show ip cef events summary

CEF table events summary:
     Storage for 10000 events (320000 bytes), 822/0 events recorded/ignored
     Matching all events, traceback depth 16
     Last event occurred 00:00:06.516 ago.
```

The following sample output is from the **show ip cef events** command displaying events that occurred within 1 second:

```
Router# show ip cef events within 1

CEF table events (storage for 10000 events, 14 events recorded)
+00:00:00.000:[Default-table] *.*.*.*/*          New FIB table          [OK]
+00:00:00.000:[Default-table] 9.1.80.194/32      FIB insert in mtrie    [OK]
+00:00:00.000:[Default-table] 9.1.80.0/32        FIB insert in mtrie    [OK]
+00:00:00.000:[Default-table] 9.1.80.255/32      FIB insert in mtrie    [OK]
+00:00:00.004:[Default-table] 9.1.80.0/24        FIB insert in mtrie    [OK]
```

```
+00:00:00.004:[Default-table] 9.1.80.0/24        NBD up                [OK]
+00:00:00.004:[Default-table] 224.0.0.0/4        FIB insert in mtrie   [OK]
+00:00:00.012:[Default-table] 9.1.80.0/24        NBD up                [Ignr]
+00:00:00.012:[Default-table] 224.0.0.0/4        FIB remove            [OK]
+00:00:00.016:[Default-table] 224.0.0.0/4        FIB insert in mtrie   [OK]
+00:00:05.012:[Default-table] 224.0.0.0/4        FIB remove            [OK]
+00:00:05.012:[Default-table] 224.0.0.0/4        FIB insert in mtrie   [OK]
+00:00:28.440:[Default-table] 224.0.0.0/4        FIB remove            [OK]
+00:00:28.440:[Default-table] 224.0.0.0/4        FIB insert in mtrie   [OK]
First event occured at 00:00:36.568 (00:04:40.756 ago)
Last event occured at 00:01:05.008 (00:04:12.316 ago)
```

Table 34 describes the significant fields shown in the display.

Table 34 show ip cef events Field Descriptions

Field	Description
+00:00:00.000	Time stamp of the IP CEF event.
[Default-table]	Type of VPN routing and forwarding (VRF) table for this event entry.
`*.*.*.*/*`	All IP prefixes.
9.1.80.194/32	IP prefix associated with the event.
FIB insert in mtrie	IP prefix insert in the FIB table event.
NBD up	IP prefix up event.
FIB remove	FIB entry remove event.
[Ignr]	CEF ignored event.
[OK]	CEF processed event.

Related Commands

Command	Description
IP cef table consistency-check	Enables CEF table consistency checker types and parameters.
ip cef table event-log	Controls CEF table event-log characteristics.

show ip cef exact-route

To display the exact route for a source-destination IP address pair, use the **show ip cef exact-route** command in EXEC mode.

show ip cef [**vrf** *vrf-name*] **exact-route** *source-address destination-address*

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
source-address	Specifies the network source address.
destination-address	Specifies the network destination address.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)T	This command was introduced.

Usage Guidelines

When you are load balancing per destination, this command shows the exact next hop that is used for a given IP source-destination pair.

Examples

The following sample output is from the **show ip cef exact-route** command:

```
Router# show ip cef exact-route 1.1.1.1 172.17.249.252

1.1.1.1         -> 172.17.249.252 :Ethernet2/0/0 (next hop 9.1.104.1)
```

Table 35 describes the significant fields shown in the display.

Table 35 show ip cef exact-route Field Descriptions

Field	Description
1.1.1.1 -> 172.17.249.252	From source 1.1.1.1 to destination 172.17.249.252.
Ethernet2/0/0 (next hop 9.1.104.1)	Next hop is 9.1.104.1 on Ethernet 2/0/0.

show ip cef inconsistency

To display Cisco Express Forwarding (CEF) IP prefix inconsistencies, use the **show ip cef inconsistency** command in EXEC mode.

show ip cef [**vrf** *vrf-name*] **inconsistency** [**records** [**detail**]]

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
records	(Optional) Displays all recorded inconsistencies.
detail	(Optional) Displays detailed information for each CEF table entry.

Command Modes

EXEC

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command is available only on routers with line cards.

This command displays recorded CEF inconsistency records found by the lc-detect, scan-rp, scan-rib, and scan-lc detection mechanisms.

You can configure the CEF consistency detection mechanisms using the **ip cef table consistency-check** command.

Examples

The following sample output is from the **show ip cef inconsistency** command:

```
Router# show ip cef inconsistency

Table consistency checkers (settle time 65s)
 lc-detect:running
  0/0/0 queries sent/ignored/received
 scan-lc:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
 scan-rp:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
 scan-rib:running [1000 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
Inconsistencies:0 confirmed, 0/16 recorded
```

Table 36 describes the significant fields shown in the display.

Table 36 show ip cef inconsistency Field Descriptions

Field	Description
settle time	Time after a recorded inconsistency is confirmed.
lc-detect running	Consistency checker lc-detect is running.
0/0/0 queries	Number of queries sent, ignored, and received.
Inconsistencies:0 confirmed, 0/16 recorded	Number of inconsistencies confirmed, and recorded. Sixteen is the maximum number of inconsistency records to be recorded.

Related Commands

Command	Description
IP cef table consistency-check	Enables CEF table consistency checker types and parameters.

show ip cef traffic prefix-length

To display Cisco Express Forwarding (CEF) traffic statistics, use the **show ip cef traffic prefix-length** command in EXEC mode.

show ip cef [**vrf** *vrf-name*] **traffic prefix-length**

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
prefix-length	Displays traffic statistics by prefix size.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.
12.0(5)T	The **vrf** keyword was added.

Usage Guidelines

This command is used to display CEF switched traffic statistics by destination prefix length. The **ip cef accounting prefix-length** command must be enabled for the counters to increment.

Examples

The following sample output is from the **show ip cef traffic prefix-length** command:

```
Router# show ip cef traffic prefix-length

IP prefix length switching statistics:
----------------------------------------
Prefix       Number of       Number of
Length       Packets         Bytes
----------------------------------------
     0               0               0
     1               0               0
     2               0               0
     3               0               0
     4               0               0
     5               0               0
.
.
.
    28               0               0
    29               0               0
    30               0               0
    31               0               0
    32               0               0
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip cef traffic prefix-length Field Descriptions

Field	Description
Prefix Length	Destination IP prefix length for CEF switched traffic.
Number of packets	Number of packets forwarded for the specified IP prefix length.
Number of bytes	Number of bytes transmitted for the specified IP prefix length.

Related Commands

Command	Description
ip cef accounting	Enables network accounting of CEF.

show ip explicit-paths

To display the configured IP explicit paths, use the **show ip explicit-paths** EXEC command. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

show ip explicit-paths [{**name** *word* | **identifier** *number*}] [**detail**]

Syntax Description

name *word*	(Optional) Name of the explicit path.
identifier *number*	(Optional) 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.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

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 3.3.28.3
    2: next-address 3.3.27.3
```

Table 38 describes the significant fields displayed in the output.

Table 38 show ip explicit-paths Field Descriptions

Field	Description
PATH	Path name 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. Commands might be renumbered as a result.
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.

Command	Description
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.

show ip flow export

To display the statistics for the data export, including the main cache and all other enabled caches, use the **show ip flow export** command in user EXEC or privileged EXEC mode.

show ip flow export [**template**]

Syntax Description

template	(Optional) Shows the data export statistics (such as template timeout and refresh rate) for the template-specific configurations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(2)T	This command was modified to display multiple NetFlow export destinations.
12.0(24)S	The **template** keyword was added.
12.3(1)	This command was integrated into Cisco IOS Release 12.3(1).

Examples

The following is sample output from the **show ip flow export** command:

```
Router# show ip flow export

Flow export v5 is enabled for main cache
  Exporting flows to 10.51.12.4 (9991) 10.1.97.50 (9111)
  Exporting using source IP address 9.1.97.17
  Version 5 flow records
  11 flows exported in 8 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
  0 export packets were dropped due to output drops
```

Table 39 describes the significant fields shown in the display.

Table 39 show ip flow export Field Descriptions

Field	Description
Exporting flows to 10.51.12.4 (9991) 10.1.97.50 (9111)	Specifies the export destinations and ports. The ports are in parentheses.
Exporting using source IP address 9.1.97.17	Specifies the source address or interface.
Version 5 flow records	Specifies the version of the flow.
11 flows exported in 8 udp datagrams	The total number of export packets sent, and the total number of flows contained within them.
0 flows failed due to lack of export packet	No memory was available to create an export packet.
0 export packets were sent up to process level	The packet could not be processed by CEF or by fast switching, possibly because another feature requires running on the packet.
0 export packets were dropped due to no fib 0 export packets were dropped due to adjacency issues	Indicates that CEF was unable to switch the packet or forward it up to the process level.
0 export packets were dropped due to fragmentation failures 0 export packets were dropped due to encapsulation fixup failures	Indicates that the packet was dropped because of problems constructing the IP packet.
0 export packets were dropped enqueuing for the RP 0 export packets were dropped due to IPC rate limiting	Indicates that there was a problem transferring the export packet between the RP and the line card.
0 export packets were dropped due to output drops	Indicates that the send queue was full while the packet was being transmitted.

Related Commands

Command	Description
clear adjacency	Configures aggregation cache operational parameters.
exit	Leaves aggregation cache mode.
ip flow-aggregation cache	Enables aggregation cache configuration mode.

show ip mcache

To display the contents of the IP multicast fast-switching cache, use the **show ip mcache** command in EXEC mode.

show ip mcache [*group* [*source*]]

Syntax Description

group	(Optional) Displays the fast-switching cache for the single group. The *group* argument can be either a Class D IP address or a DNS name.
source	(Optional) If the *source* argument is also specified, displays a single multicast cache entry. The *source* argument can be either a unicast IP address or a DNS name.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command on the RP.

Examples

The following is sample output from the **show ip mcache** command. This entry shows a specific source (wrn-source 204.62.246.73) sending to the World Radio Network group (224.2.143.24).

```
show ip mcache wrn wrn-source

IP Multicast Fast-Switching Cache
(204.62.246.73/32, 224.2.143.24), Fddi0, Last used: 00:00:00
  Ethernet0       MAC Header: 01005E028F1800000C1883D30800
  Ethernet1       MAC Header: 01005E028F1800000C1883D60800
  Ethernet2       MAC Header: 01005E028F1800000C1883D40800
  Ethernet3       MAC Header: 01005E028F1800000C1883D70800
```

Table 40 describes the significant fields shown in the output.

Table 40 show ip mcache Field Descriptions

Field	Description
204.62.246.73	Source address.
224.2.143.24	Destination address.
Fddi0	Incoming or expected interface on which the packet should be received.

Table 40 show ip mcache Field Descriptions (continued)

Field	Description
Last used:	Latest time the entry was accessed for a packet that was successfully fast switched: • "semi-fast" indicates that the first part of the outgoing interface list is fast switched and the rest of the list is process-level switched. • "mds" indicates that multicast distributed switching is being used instead of the fast cache. • "never" indicates that the fast cache entry is not used (it is process switched).
Ethernet0 MAC Header:	Outgoing interface list and respective MAC header that is used when rewriting the packet for output. If the interface is a tunnel, the MAC header will show the real next hop MAC header and then, in parentheses, the real interface name.

The following is sample output from the **show ip mcache** command when MDS is in effect.

```
Router# show ip mcache

IP Multicast Fast-Switching Cache
(*, 224.2.170.73), Fddi3/0/0, Last used: mds
  Tunnel3         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
  Tunnel0         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
  Tunnel1         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
```

show ip mds forwarding

On a line card, to display the MFIB table and forwarding information for multicast distributed switching (MDS), use the **show ip mds forwarding** command in EXEC mode.

show ip mds forwarding [*group-address*] [*source-address*]

Syntax Description

group-address	(Optional) Address of the IP multicast group for which to display the MFIB table.
source-address	(Optional) Address of the source of IP multicast packets for which to display the MFIB table.

Command Modes

EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.

Usage Guidelines

Use this command on the line card. This command displays the MFIB table, forwarding information, and related flags and counts.

Note To reach the console for a line card, enter **attach** *slot#* (slot number where the line card resides).

On a GSR only, line card commands can be executed from the RP using the following syntax: **execute** [**slot** *slot-number* | **all**] *command.*

The *command* argument is any of the line card **show** commands, such as **show ip mds summary** and **show ip mds forward**.

Examples

The following is sample output from the **show ip mds forwarding** command:

```
Router# show ip mds forwarding

IP multicast MDFS forwarding information and statistics:
Flags: N - Not MDFS switchable, F - Not all MDFS switchable, O - OIF Null
       R - In-ratelimit, A - In-access, M - MTU mismatch, P - Register set

Interface state: Interface, Next-Hop, Mac header

(*, 224.2.170.73),
  Incoming interface: Null
  Pkts: 0, last used: never, Kbps: 0, fast-flags: N
  Outgoing interface list: Null

(128.97.62.86, 224.2.170.73) [31]
  Incoming interface: Fddi3/0/0
  Pkts: 3034, last used: 00:00:00, Kbps: 0, fast-flags: M
  Outgoing interface list:
```

Table 41 describes the significant fields shown in the output.

Table 41 show ip mds forwarding Field Descriptions

Field	Description
(128.97.62.86, 224.2.170.73) [31])	Source and group addresses. The number in brackets is the hash bucket for the route.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
Pkts	Total number of packets switched by that entry.
last used:	Time when this MFIB entry was used to switch a packet.
Kbps:	Kilobits per second of the switched traffic.
Outgoing interface list:	Interfaces through which packets will be forwarded.

show ip mds interface

To display the status of multicast distributed switching (MDS) interfaces, use the **show ip mds interface** command in EXEC mode.

show ip mds interface

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.

Usage Guidelines

Use this command on the RP.

Examples

The following is sample output from the **show ip mds interface** command:

```
Router# show ip mds interface

Ethernet1/0/0 is up, line protocol is up
Ethernet1/0/1 is up, line protocol is up
Fddi3/0/0 is up, line protocol is up
FastEthernet3/1/0 is up, line protocol is up
```

Table 42 describes the significant fields in the output.

Table 42 show ip mds interface Field Descriptions

Field	Description
Ethernet1/0/0 is up	Status of interface.
line protocol is up	Status of line protocol.

show ip mds stats

To display switching statistics or line card statistics for multicast distributed switching (MDS), use the **show ip mds stats** command in EXEC mode.

show ip mds stats [**switching** | **linecard**]

Syntax Description

switching	(Optional) Displays switching statistics.
linecard	(Optional) Displays line card statistics.

Command Modes

EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.

Usage Guidelines

Use this command on the RP.

Examples

The following is sample output from the **show ip mds stats** command used with the **switching** keyword:

```
Router# show ip mds stats switching

Slot Total       Switched    Drops       RPF         Punts       Failures
                                                                 (switch/clone)
 1   0           0           0           0           4           0/0
 3   20260925    18014717    253         93          2247454     1/0
```

Table 43 describes the significant fields in the output.

Table 43 show ip mds stats switching Field Descriptions

Field	Description
Slot	Slot number for the line card.
Total	Total number of packets received.
Switched	Total number of packets switched.
Drops	Total number of packets dropped.
RPF	Total number of packets that failed RPF lookup.
Punts	Total number of packets sent to the RP because the line card could not switch them.
Failures (switch/clone)	Times that the RP tried to switch but failed because of lack of resources or clone for the RSP only; failed to get a packet clone.

The following is sample output from the **show ip mds stats** command with the **linecard** keyword:

```
Router# show ip mds stats linecard

Slot      Status    IPC(seq/max) Q(high/route)  Reloads
 1        active    10560/10596      0/0            9
 3        active    11055/11091      0/0            9
```

show ip mds summary

To display a summary of the MFIB table for multicast distributed switching (MDS), use the **show ip mds summary** command in EXEC mode.

show ip mds summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.

Usage Guidelines

Use this command on a line card. On a GSR only, line card commands can be executed from the RP using the following syntax:

execute [**slot** *slot-number* | **all**] *command*

The *command* argument is any of the line card **show** commands, such as **show ip mds summary** and **show ip mds forward**.

Examples

The following is sample output from the **show ip mds summary** command:

```
Router# show ip mds summary

IP multicast MDFS forwarding information and statistics:
Flags: N - Not MDFS switchable, F - Not all MDFS switchable, O - OIF Null
       R - In-ratelimit, A - In-access, M - MTU mismatch, P - Register set

Interface state: Interface, Next-Hop, Mac header

(*, 224.2.170.73),
  Incoming interface: Null
  Pkts: 0, last used: never, Kbps: 0, fast-flags: N
(128.97.62.86, 224.2.170.73) [31]
  Incoming interface: Fddi3/0/0
  Pkts: 3045, last used: 00:00:03, Kbps: 0, fast-flags: M
(128.223.3.7, 224.2.170.73) [334]
  Incoming interface: Fddi3/0/0
  Pkts: 0, last used: never, Kbps: 0, fast-flags: M
```

Table 44 describes the significant fields in the output.

Table 44 show ip mds summary Field Descriptions

Field	Description
(128.97.62.86, 224.2.170.73) [31]	Source and group addresses. The number in brackets is the hash bucket for the route.
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
Pkts	Total number of packets switched by that entry.
last used	Time when this MFIB entry was used to switch a packet.
Kbps	Kilobits per second of the switched traffic.

show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** command in EXEC mode.

show ip mroute [*group-name* | *group-address*] [*source*] [**summary**] [**count**] [**active** *kbps*]

Syntax Description

group-name | *group-address*	(Optional) IP address, name, or interface of the multicast group as defined in the DNS hosts table.
source	(Optional) IP address or name of a multicast source.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
active *kbps*	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at a rate of *kbps* or higher. The *kbps* argument defaults to 4.

Defaults

The **show ip mroute** command displays all groups and sources.
The **show ip mroute active** command displays all sources sending at a rate greater than or equal to 4 kbps.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The flag "H" was added in the output display to indicate that an outgoing interface is hardware-switched in the case of IP multicast Multilayer Switching (MLS).

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP multicast routing table.

The Cisco IOS software populates the multicast routing table by creating source, group (S, G) entries from star, group (*, G) entries. The star (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Examples

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This command displays the contents of the IP multicast routing table for the multicast group named cbone-audio.

```
Router# show ip mroute cbone-audio

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 0.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 0.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(198.92.37.100/32, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 198.92.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(198.92.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

The following is sample output from the **show ip mroute** command that shows the VCD value, because an ATM interface with PIM multipoint signalling is enabled:

```
Router# show ip mroute 224.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:03:57/00:02:54, RP 130.4.101.1, flags: SJ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    ATM0/0, VCD 14, Forward/Sparse, 00:03:57/00:02:53
```

The following is sample output from the **show ip mroute** command with the **summary** keyword:

```
Router# show ip mroute summary

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop, State/Mode

(*, 224.255.255.255), 2d16h/00:02:30, RP 171.69.10.13, flags: SJPC

(*, 224.2.127.253), 00:58:18/00:02:00, RP 171.69.10.13, flags: SJC

(*, 224.1.127.255), 00:58:21/00:02:03, RP 171.69.10.13, flags: SJC

(*, 224.2.127.254), 2d16h/00:00:00, RP 171.69.10.13, flags: SJCL
  (128.9.160.67/32, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
  (129.48.244.217/32, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
  (130.207.8.33/32, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
  (131.243.2.62/32, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
  (140.173.8.3/32, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
  (171.69.60.189/32, 224.2.127.254), 00:03:47/00:00:46, flags: CLJT
```

The following is sample output from the **show ip mroute** command with the **active** keyword:

```
Router# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 146.137.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

The following example of the **show ip mroute** EXEC command is displayed when IP multicast MLS is configured. Note that the "H" indicates hardware switched.

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT, H - Hardware
switched
Timers: Uptime/Expires

(*, 229.10.0.1), 00:04:35/00:02:59, RP 0.0.0.0, flags: DJC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
 Vlan6, Forward/Dense, 00:00:30/00:02:30
    Vlan5, Forward/Dense, 00:04:35/00:02:30
    Vlan2, Forward/Dense, 00:01:28/00:00:00

(192.0.2.20, 229.10.0.1), 00:04:35/00:02:27, flags: CT
Incoming interface: Vlan2, RPF nbr 0.0.0.0
Outgoing interface list:
    Vlan5, Forward/Dense, 00:03:25/00:00:00, H
    Vlan6, Forward/Dense, 00:00:10/00:00:00, H
```

Table 45 describes the significant fields shown in the output.

Table 45 show ip mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
C - Connected	A member of the multicast group is present on the directly connected interface.
L - Local	The router itself is a member of the multicast group.
P - Pruned	Route has been pruned. The Cisco IOS software keeps this information in case a downstream member wants to join the source.
R - RP-bit set	Indicates that the (S, G) entry is pointing toward the rendezvous point (RP). The RP is typically a prune state along the shared tree for a particular source.
F - Register flag	Indicates that the software is registering for a multicast source.
T - SPT-bit set	Indicates that packets have been received on the shortest path source tree.
H - Hardware switched	Indicates the outgoing interface is hardware switched because IP multicast MLS is enabled.
Timers:	Uptime/Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.
(*, 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or “star comma G” entries. Entries in the second format are referred to as (S, G) or “S comma G” entries. (*, G) entries are used to build (S, G) entries.
uptime	How long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table.
expires	How long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table on the outgoing interface.
RP	Address of the rendezvous point router. For routers and access servers operating in sparse mode, this address is always 0.0.0.0.
flags:	Information about the entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor	IP address of the upstream router to the source. “Tunneling” indicates that this router is sending data to the rendezvous point encapsulated in Register packets. The hexadecimal number in parentheses indicates to which rendezvous point it is registering. Each bit indicates a different rendezvous point if multiple rendezvous points per group are used.

Table 45 show ip mroute Field Descriptions (continued)

Field	Description
Dvmrp or Mroute	Indicates whether the RPF information is obtained from the DVMRP routing table or the static mroutes configuration.
Outgoing interface list:	Interfaces through which packets will be forwarded. When the **ip pim nbma-mode** command is enabled on the interface, the IP address of the PIM neighbor is also displayed.
Ethernet0	Name and number of the outgoing interface.
Next hop or VCD	Next hop specifies the IP address of the downstream neighbors. VCD is the virtual circuit descriptor number. VCD0 means the group is using the static-map virtual circuit.
Forward/Dense	Indicates that packets will be forwarded on the interface if there are no restrictions due to access lists or TTL threshold. Following the slash (/) is the mode in which the interface is operating (dense or sparse).
Forward/Sparse	Sparse mode interface is in forward mode.
<*time/time*> (uptime/expiration time)	Per interface, how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Following the slash (/) is how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.

The following is sample output from the **show ip mroute** command with the **count** keyword:

```
Router# show ip mroute count

IP Multicast Statistics
4045 routes using 2280688 bytes of memory
41 groups, 97.65 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:239.0.18.1, Source count:200, Packets forwarded:348232, Packets received:348551
  RP-tree:Forwarding:12/0/218/0, Other:12/0/0
  Source:10.1.1.1/32, Forwarding:1763/1/776/9, Other:1764/0/1
  Source:10.1.1.2/32, Forwarding:1763/1/777/9, Other:1764/0/1
  Source:10.1.1.3/32, Forwarding:1763/1/783/10, Other:1764/0/1
  Source:10.1.1.4/32, Forwarding:1762/1/789/10, Other:1763/0/1
  Source:10.1.1.5/32, Forwarding:1762/1/768/10, Other:1763/0/1
  Source:10.1.1.6/32, Forwarding:1793/1/778/10, Other:1794/0/1
  Source:10.1.1.7/32, Forwarding:1793/1/763/10, Other:1794/0/1
  Source:10.1.1.8/32, Forwarding:1793/1/785/10, Other:1794/0/1
  Source:10.1.1.9/32, Forwarding:1793/1/764/9, Other:1794/0/1
  Source:10.1.1.10/32, Forwarding:1791/1/774/10, Other:1792/0/1
  Source:10.1.2.1/32, Forwarding:1689/1/780/10, Other:1691/0/2
  Source:10.1.2.2/32, Forwarding:1689/1/782/10, Other:1691/0/2
  Source:10.1.2.3/32, Forwarding:1689/1/776/9, Other:1691/0/2
.
.
.

Group:239.0.18.132, Source count:0, Packets forwarded:8810, Packets received:8810
  RP-tree:Forwarding:8810/7/780/49, Other:8810/0/0

Group:239.0.17.132, Source count:0, Packets forwarded:704491, Packets received:704491
  RP-tree:Forwarding:704491/639/782/4009, Other:704491/0/0

Group:239.0.17.133, Source count:0, Packets forwarded:704441, Packets received:704441
  RP-tree:Forwarding:704441/639/782/3988, Other:704441/0/0

Group:239.0.18.133, Source count:0, Packets forwarded:8810, Packets received:8810
  RP-tree:Forwarding:8810/8/786/49, Other:8810/0/0

Group:239.0.18.193, Source count:0, Packets forwarded:0, Packets received:0

Group:239.0.17.193, Source count:0, Packets forwarded:0, Packets received:0

Group:239.0.18.134, Source count:0, Packets forwarded:8803, Packets received:8803
  RP-tree:Forwarding:8803/8/774/49, Other:8803/0/0
```

Note The RP-tree: field is displayed only for non-Source Specific Multicast (SSM) groups that have a (*, G) entry and a positive packet received count.

Table 46 describes the significant fields shown in the display.

Table 46 show ip mroute count Field Descriptions

Field	Description
Group:	Summary statistics for traffic on an IP multicast group G. This row is displayed only for non-SSM groups.
Forwarding Counts:	Statistics on the packets that are received and forwarded to at least one interface. **Note** There is no specific command to clear only the forwarding counters; you can clear only the actual multicast forwarding state with the **clear ip mroute** command. Issuing this command will cause interruption of traffic forwarding.
Pkt Count/	Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created.
Pkts per second/	Number of packets received and forwarded per second. On an IP multicast fast-switching platform, this number is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kilobits per second	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Total/	Total number of packets received.
RPF failed/	Number of packets not forwarded due to a failed RPF or acceptance check (when bidir-PIM is configured).
Other drops(OIF-null, rate-limit etc)	Number of packets not forwarded for reasons other than an RPF or acceptance check (such as the OIF list was empty or because the packets were discarded because of a configuration, such as **ip multicast rate-limit**, was enabled).
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For SSM range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.

Table 46 show ip mroute count Field Descriptions (continued)

Field	Description
Source count:	Number of (S, G) states for this group G. Individual (S, G) counters are detailed in the Source: output field rows.
Packets forwarded:	The sum of the packets detailed in the Forwarding Counts: fields for this IP multicast group G. This field is the sum of the RP-tree and all Source: fields for this group G.
Packets received:	The sum of packets detailed in the Other counts fields for this IP multicast group G. This field is the sum of the Other count: Pkt Count fields of the RP-tree: and Source: rows for this group G.
RP-tree:	Counters for the (*, G) state of this group G. These counters are displayed only for groups that have a forwarding mode that do not forward packets on the shared tree. These (*,G) groups are bidir-PIM and PIM-SM groups. There are no RP-tree displays for PIM-DM and SSM range groups.
Source:	Counters for an individual (S, G) state of this group G. There are no (S, G) states for bidir-PIM groups.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip pim	Enables PIM on an interface.

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** EXEC command.

show ip ospf database opaque-area

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(8)S	This command was introduced.

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 (25.3.3.3) (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: 1.0.0.0
  Opaque Type: 1
  Opaque ID: 0
  Advertising Router: 24.8.8.8
  LS Seq Number: 80000004
  Checksum: 0xD423
  Length: 132
  Fragment number : 0

    MPLS TE router ID: 24.8.8.8

    Link connected to Point-to-Point network
      Link ID : 26.2.2.2

      Interface Address : 198.1.1.1
```

Table 47 describes the significant fields displayed in the output.

Table 47 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 traffic-eng

To display information about the links available on the local router for traffic engineering, use the **show ip ospf mpls traffic-eng** EXEC command.

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 the 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

EXEC

Command History

Release	Modification
Release 12.0 S	This command was introduced.

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 (23.0.0.1) (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 :66.0.0.1
      Neighbor Address :66.0.0.2
      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 :195.1.1.2
```

```
Interface Address :195.1.1.1
Neighbor Address :195.1.1.2
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 48 describes the significant fields shown in the output.

Table 48 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** interface configuration command.
Maximum reservable bandwidth	Bandwidth available for traffic engineering on this link. This value is set in the **ip rsvp** interface configuration command.
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 pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** command in EXEC mode.

show ip pim interface [*type number*] [**count**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
count	(Optional) Number of packets received and sent out the interface.

Command Modes

EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.
12.0(5)T	The flag "H" was added in the output display to indicate that an outgoing interface is hardware-switched in the case of IP multicast Multilayer Switching (MLS).

Usage Guidelines

This command works only on interfaces that are configured for PIM.

Examples

The following is sample output from the **show ip pim interface** EXEC command:

```
router# show ip pim interface

Address          Interface          Mode    Neighbor  Query     DR
                                            Count     Interval
198.92.37.6      Ethernet0          Dense   2         30        198.92.37.33
198.92.36.129    Ethernet1          Dense   2         30        198.92.36.131
10.1.37.2        Tunnel0            Dense   1         30        0.0.0.0
```

The following is sample output from the **show ip pim interface** command with the **count** keyword:

```
router# show ip pim interface count

Address          Interface          FS  Mpackets In/Out
171.69.121.35    Ethernet0          *   548305239/13744856
171.69.121.35    Serial0.33         *   8256/67052912
198.92.12.73     Serial0.1719       *   219444/862191
```

The following is sample output from the **show ip pim interface** command with the **count** keyword when IP multicast MLS is enabled. The examples lists the PIM interfaces that are fast switched and process switched, and the packet counts for these. The "H" is added to interfaces where IP multicast MLS is enabled.

```
router# show ip pim interface count

States: FS - Fast Switched, H - Hardware Switched
```

```
Address          Interface          FS  Mpackets In/Out
192.1.10.2       Vlan10             * H 40886/0
192.1.11.2       Vlan11             * H 0/40554
192.1.12.2       Vlan12             * H 0/40554
192.1.23.2       Vlan23             *   0/0
192.1.24.2       Vlan24             *   0/0
```

Table 49 describes the significant fields shown in the output.

Table 49 show ip pim interface count Field Descriptions

Field	Description
Address	IP address of the next hop router.
Interface	Interface type and number that is configured to run PIM.
Mode	Multicast mode in which the Cisco IOS software is operating. This can be dense mode or sparse mode. DVMRP indicates that a DVMRP tunnel is configured.
Neighbor Count	Number of PIM neighbors that have been discovered through this interface. If the neighbor count is 1 for a DVMRP tunnel, the neighbor is active (receiving probes and reports).
Query Interval	Frequency (in seconds) of PIM router query messages, as set by the **ip pim query-interval** interface configuration command. The default is 30 seconds.
DR	IP address of the designated router on the LAN. Note that serial lines do not have designated routers, so the IP address is shown as 0.0.0.0.
FS	An asterisk (*) in this column indicates that fast switching is enabled.
Mpackets In/Out	Number of packets into and out of the interface since the box has been up.

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

show ip protocols vrf

To display the routing protocol information associated with a VRF, use the **show ip protocols vrf** command in EXEC mode.

show ip protocols vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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 vpn2

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
    13.13.13.13          200      02:20:54
    18.18.18.18          200      03:26:15
  Distance:external 20 internal 200 local 200
```

Table 50 describes the significant fields shown in the output.

Table 50 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 vrf

To display the IP routing table associated with a VRF, use the **show ip route vrf** command in EXEC mode.

show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]]

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.
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.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

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    51.0.0.0/8 [200/0] via 13.13.13.13, 00:24:19
C    50.0.0.0/8 is directly connected, Ethernet1/3
B    11.0.0.0/8 [20/0] via 50.0.0.1, 02:10:22
B    12.0.0.0/8 [200/0] via 13.13.13.13, 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  51.0.0.0/8 [200/0] via 13.13.13.13, 03:44:14
B  11.0.0.0/8 [20/0] via 51.0.0.1, 03:44:12
B  12.0.0.0/8 [200/0] via 13.13.13.13, 03:43:14
```

Related Commands

Command	Description
show ip cache	Displays the CEF forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip rsvp host

To display RSVP terminal point information for receivers or senders, use the **show ip rsvp host** EXEC command.

show ip rsvp host {**senders** | **receivers**} [*hostname* | *A.B.C.D*]

Syntax Description

senders	Displays information for senders.
receivers	Displays information for receivers.
hostname	(Optional) Restricts the display to sessions with *hostname* as their destination.
A.B.C.D	(Optional) Restricts the display to sessions with the specified IP address as their destination.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show ip rsvp host receivers** command:

```
Router# show ip rsvp host receivers

To            From          Pro DPort Sport Next Hop      I/F   Fi Serv BPS Bytes
10.0.0.11     10.1.0.4      0   10011 1                         SE LOAD 100K  1K
```

Table 51 describes the significant fields shown in the output.

Table 51 show ip rsvp host Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code.
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (wild card, shared explicit, or fixed).

Table 51 show ip rsvp host Field Descriptions (continued)

Field	Description
Serv	Service (RATE or LOAD).
BPS	Reservation rate (in bits per second).
Bytes	Bytes of requested burst size.

Related Commands

Command	Description
show ip rsvp request	Displays the RSVP reservations currently being requested upstream for a specified interface or all interfaces.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP-related sender information currently in the database.

show ip vrf

To display the set of defined VRFs and associated interfaces, use the **show ip vrf** command in EXEC mode.

show ip vrf [{**brief** | **detail** | **interfaces**}] [*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.
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 optional parameters are specified the command shows concise information about all configured VRFs.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to display information about VRFs. Two levels of detail are available: use the **brief** keyword or no keyword to display concise information, or use the **detail** keyword to display all information. To display information about all interfaces bound to a particular VRF, or to any VRF, use the **interfaces** keyword.

Examples

This example shows brief information for the VRFs currently configured:

```
Router# show ip vrf

  Name                Default RD          Interfaces
  vrf1                100:1               Ethernet1/3
  vrf2                100:2               Ethernet0/3
```

Table 52 describes the fields shown in this example.

Table 52 show ip vrf Field Descriptions

Field	Description
Name	Specifies the VRF name.
Default RD	Specifies the default route distinguisher.
Interfaces	Specifies the network interfaces.

This example shows detailed information for the VRF called vrf1:

```
Router# show ip vrf detail vrf1

VRF vrf1; default RD 100:1
 Interfaces:
  Ethernet1/3
 Connected addresses are in global routing table
 Export VPN route-target communities
  RT:100:1
 Import VPN route-target communities
  RT:100:1
 No import route-map
```

Table 53 describes the significant fields shown in the output.

Table 53 show ip vrf detail Field Descriptions

Field	Description
Interfaces	Specifies the network interfaces.
Export	Specifies VPN route-target export communities.
Import	Specifies VPN route-target import communities.

This example shows the interfaces bound to a particular VRF:

```
Router# show ip vrf interfaces

Interface       IP-Address      VRF                             Protocol
Ethernet2       130.22.0.33     blue_vrf                        up
Ethernet4       130.77.0.33     hub                             up
router#
```

Table 54 describes the significant fields shown in the output.

Table 54 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/down) for each VRF interface.

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
ip vrf forwarding	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.

show isis database verbose

To display additional information about the database, use the **show isis database verbose** EXEC command.

show isis database verbose

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

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:   5.5.5.5
  IP Address:  172.21.39.5
  Metric:10         IP 172.21.39.0/24
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 55 describes the fields displayed in this example.

Table 55 show isis database verbose Field Descriptions

Field	Description
LSPID	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 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	Host name 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 55 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.

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 traffic-eng adjacency-log

To display a log of 20 entries of MPLS traffic engineering IS-IS adjacency changes, use the **show isis mpls traffic-eng adjacency-log** EXEC command.

show isis mpls traffic-eng adjacency-log

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

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  170.1.1.2        PO1/0/0   Up     level-1
04:52:37  0000.0024.0004.02  0.0.0.0          Et0/2     Up     level-1
```

Table 56 describes the significant fields shown in the output.

Table 56 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 MPLS traffic engineering, use the **show isis mpls traffic-eng advertisements** EXEC command.

show isis mpls traffic-eng advertisements

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

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:5.5.5.5
  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 57 describes the significant fields shown in the output.

Table 57 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.

Table 57 show isis mpls traffic-eng advertisements Field Descriptions (continued)

Field	Description
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 IS-IS next hop calculation, use the **show isis mpls traffic-eng tunnel** EXEC command.

show isis mpls traffic-eng tunnel

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.0(5)	This command was introduced.

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         2.2.2.2       -3       Relative
                    Tunnel1021    10000        2.2.2.2       11       Absolute
tomklong-route.00   Tunnel1031    10000        3.3.3.3       -1       Relative
                    Tunnel1032    10000        3.3.3.3
```

Table 58 describes the significant fields shown in the output.

Table 58 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 lane

To display detailed information for all the LANE components configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane** command in EXEC mode.

AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

show lane [**interface atm** *slot/port*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

ATM Port Adapter on the Cisco 7500 Series Routers

show lane [**interface atm** *slot/port-adapter/port*[**.***subinterface-number*] | **name** *elan-name*][**brief**]

Cisco 4500 and 4700 Routers

show lane [**interface atm** *number*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

Syntax Description

interface atm *slot/port*	(Optional) ATM interface slot and port for the following: • AIP on the Cisco 7500 series routers. • ATM port adapter on the Cisco 7200 series routers.
interface atm *slot/port-adapter/port*	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
interface atm *number*	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
.*subinterface-number*	(Optional) Subinterface number.
name *elan-name*	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.
brief	(Optional) Keyword used to display the brief subset of available information.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Using the **show lane** command is equivalent to using the **show lane config**, **show lane server**, **show lane bus**, and **show lane client** commands. The **show lane** command shows all LANE-related information except the **show lane database** command information.

Examples

The following is sample output from the **show lane** command for an Ethernet ELAN:

```
Router# show lane

LE Config Server ATM2/0 config table: cisco_eng
Admin: up  State: operational
LECS Mastership State: active master
list of global LECS addresses (30 seconds to update):
39.020304050607080910111213.00000CA05B43.00  <-------- me
ATM Address of this LECS: 39.020304050607080910111213.00000CA05B43.00 (auto)
 vcd  rxCnt txCnt  callingParty
  50      2      2  39.020304050607080910111213.00000CA05B41.02 LES elan2 0 active
cumulative total number of unrecognized packets received so far: 0
cumulative total number of config requests received so far: 30
cumulative total number of config failures so far: 12
    cause of last failure: no configuration
    culprit for the last failure: 39.020304050607080910111213.00602F557940.01

LE Server ATM2/0.2  ELAN name: elan2  Admin: up  State: operational
type: ethernet         Max Frame Size: 1516
ATM address: 39.020304050607080910111213.00000CA05B41.02
LECS used: 39.020304050607080910111213.00000CA05B43.00 connected, vcd 51
control distribute: vcd 57, 2 members, 2 packets

proxy/ (ST: Init, Conn, Waiting, Adding, Joined, Operational, Reject, Term)
lecid ST vcd    pkts Hardware Addr  ATM Address
   1  O   54       2 0000.0ca0.5b40 39.020304050607080910111213.00000CA05B40.02
   2  O   81       2 0060.2f55.7940 39.020304050607080910111213.00602F557940.02

LE BUS ATM2/0.2  ELAN name: elan2  Admin: up  State: operational
type: ethernet         Max Frame Size: 1516
ATM address: 39.020304050607080910111213.00000CA05B42.02
data forward: vcd 61, 2 members, 0 packets, 0 unicasts

lecid  vcd     pkts   ATM Address
    1   58        0 39.020304050607080910111213.00000CA05B40.02
    2   82        0 39.020304050607080910111213.00602F557940.02

LE Client ATM2/0.2  ELAN name: elan2  Admin: up  State: operational
Client ID: 1                LEC up for 11 minutes 49 seconds
Join Attempt: 1
HW Address: 0000.0ca0.5b40   Type: ethernet             Max Frame Size: 1516

ATM Address: 39.020304050607080910111213.00000CA05B40.02

 VCD  rxFrames  txFrames  Type       ATM Address
   0         0         0  configure  39.020304050607080910111213.00000CA05B43.00
  55         1         4  direct     39.020304050607080910111213.00000CA05B41.02
  56         6         0  distribute 39.020304050607080910111213.00000CA05B41.02
  59         0         1  send       39.020304050607080910111213.00000CA05B42.02
  60         3         0  forward    39.020304050607080910111213.00000CA05B42.02
  84         3         5  data       39.020304050607080910111213.00602F557940.02
```

The following is sample output from the **show lane** command for a Token Ring LANE network:

```
Router# show lane

LE Config Server ATM4/0 config table: eng
Admin: up  State: operational
LECS Mastership State: active master
list of global LECS addresses (35 seconds to update):
39.020304050607080910111213.006047704183.00  <-------- me
ATM Address of this LECS: 39.020304050607080910111213.006047704183.00 (auto)
 vcd  rxCnt  txCnt  callingParty
```

```
   7      1      1  39.020304050607080910111213.006047704181.01 LES elan1 0 active
cumulative total number of unrecognized packets received so far: 0
cumulative total number of config requests received so far: 2
cumulative total number of config failures so far: 0

LE Server ATM4/0.1  ELAN name: elan1  Admin: up  State: operational
type: token ring         Max Frame Size: 4544      Segment ID: 2048
ATM address: 39.020304050607080910111213.006047704181.01
LECS used: 39.020304050607080910111213.006047704183.00 connected, vcd 9
control distribute: vcd 12, 1 members, 2 packets

proxy/ (ST: Init, Conn, Waiting, Adding, Joined, Operational, Reject, Term)
lecid ST vcd    pkts Hardware Addr  ATM Address
   1  O    8       3 100.2         39.020304050607080910111213.006047704180.01
                     0060.4770.4180 39.020304050607080910111213.006047704180.01

LE BUS ATM4/0.1  ELAN name: elan1  Admin: up  State: operational
type: token ring         Max Frame Size: 4544      Segment ID: 2048
ATM address: 39.020304050607080910111213.006047704182.01
data forward: vcd 16, 1 members, 0 packets, 0 unicasts

lecid  vcd     pkts   ATM Address
    1   13        0 39.020304050607080910111213.006047704180.01

LE Client ATM4/0.1  ELAN name: elan1  Admin: up  State: operational
Client ID: 1                LEC up for 2 hours 25 minutes 39 seconds
Join Attempt: 3
HW Address: 0060.4770.4180   Type: token ring           Max Frame Size: 4544
Ring:100    Bridge:2        ELAN Segment ID: 2048
ATM Address: 39.020304050607080910111213.006047704180.01

 VCD  rxFrames  txFrames  Type       ATM Address
   0         0         0  configure  39.020304050607080910111213.006047704183.00
  10         1         3  direct     39.020304050607080910111213.006047704181.01
  11         2         0  distribute 39.020304050607080910111213.006047704181.01
  14         0         0  send       39.020304050607080910111213.006047704182.01
  15         0         0  forward    39.020304050607080910111213.006047704182.01
```

Table 59 describes significant fields shown in the output.

Table 59 show lane Field Descriptions

Field	Description
LE Config Server	Identifies the following lines as applying to the LANE configuration server. These lines are also displayed in output from the **show lane config** command. See the **show lane config** command for explanations of the output.
LE Server	Identifies the following lines as applying to the LANE server. These lines are also displayed in output from the **show lane server** command. See the **show lane server** command for explanations of the output.
LE BUS	Identifies the following lines as applying to the LANE broadcast and unknown server. These lines are also displayed in output from the **show lane bus** command. See the **show lane bus** command for explanations of the output.
LE Client	Identifies the following lines as applying to a LANE client. These lines are also displayed in output from the **show lane client** command. See the **show lane bus** command for explanations of the output.

show lane bus

To display detailed LANE information for the broadcast and unknown server (BUS) configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane bus** command in EXEC mode:

AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

show lane bus [**interface atm** *slot/port*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

ATM Port Adapter on the Cisco 7500 Series Routers

show lane bus [**interface atm** *slot/port-adapter/port*[**.***subinterface-number*] | **name** *elan-name*][**brief**]

Cisco 4500 and 4700 Routers

show lane bus [**interface atm** *number*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

Syntax Description

interface atm *slot/port*	(Optional) ATM interface slot and port for the following: • AIP on the Cisco 7500 series routers. • ATM port adapter on the Cisco 7200 series routers.
interface atm *slot/port-adapter/port*	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
interface atm *number*	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
.*subinterface-number*	(Optional) Subinterface number.
name *elan-name*	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.
brief	(Optional) Displays the brief subset of available information.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output from the **show lane bus** command for an Ethernet ELAN:

```
Router# show lane bus

LE BUS ATM2/0.2  ELAN name: elan2  Admin: up  State: operational
```

```
type: ethernet         Max Frame Size: 1516
ATM address: 39.020304050607080910111213.00000CA05B42.02
data forward: vcd 61, 2 members, 0 packets, 0 unicasts

lecid  vcd     pkts   ATM Address
    1   58        0 39.020304050607080910111213.00000CA05B40.02
    2   82        0 39.020304050607080910111213.00602F557940.02
```

The following is sample output from the **show lane bus** command for a Token Ring LANE:

```
show lane bus

LE BUS ATM3/0.1  ELAN name: anubis  Admin: up  State: operational
type: token ring         Max Frame Size: 4544      Segment ID: 2500
ATM address: 47.009181000000000000000000.00000CA01662.01
data forward: vcd 14, 2 members, 0 packets, 0 unicasts

lecid  vcd     pkts   ATM Address
    1   11        0 47.009181000000000000000000.00000CA01660.01
    2   17        0 47.009181000000000000000000.00000CA04960.01
```

Table 60 describes significant fields shown in the output.

Table 60 show lane bus Field Descriptions

Field	Description
LE BUS ATM2/0.2	Interface and subinterface for which information is displayed.
ELAN name	Name of the ELAN for this BUS.
Admin	Administrative state, either up or down.
State	Status of this LANE BUS. Possible states include down and operational.
type	Type of ELAN.
Max Frame Size	Maximum frame size (in bytes) on the ELAN.
Segment ID	The ring number of the ELAN. This field appears only for Token Ring LANE.
ATM address	ATM address of this LANE BUS.
data forward	Virtual channel descriptor of the Data Forward VCC, the number of LANE clients attached to the VCC, and the number of packets sent on the VCC.
lecid	Identifier assigned to each LANE client on the Data Forward VCC.
vcd	Virtual channel descriptor used to reach the LANE client.
pkts	Number of packets sent by the BUS to the LANE client.
ATM Address	ATM address of the LANE client.

show lane client

To display detailed LANE information for all the LANE clients configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane client** command in EXEC mode.

AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

show lane client detail [**interface atm** *slot/port*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

ATM Port Adapter on the Cisco 7500 Series Routers

show lane client detail [**interface atm** *slot/port-adapter/port*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

Cisco 4500 and 4700 Routers

show lane client detail [**interface atm** *number*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

Syntax Description

detail	Displays additional FSSRP information.
interface atm *slot/port*	(Optional) ATM interface slot and port for the following: • AIP on the Cisco 7500 series routers. • ATM port adapter on the Cisco 7200 series routers.
interface atm *slot/port-adapter/port*	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
interface atm *number*	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
.*subinterface-number*	(Optional) Subinterface number.
name *elan-name*	(Optional) Name of ELAN. The maximum length of the name is 32 characters.
brief	(Optional) Displays the brief subset of available information.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	The **detail** option and command output line “This client is running in FSSRP mode” were added.

Examples

The following is sample output from the **show lane client** command for an Ethernet ELAN:

```
Router# show lane client

LE Client ATM2/0.2  ELAN name: elan2  Admin: up  State: operational
Client ID: 1                LEC up for 11 minutes 49 seconds
Join Attempt: 1
HW Address: 0000.0ca0.5b40   Type: ethernet             Max Frame Size: 1516

ATM Address: 39.020304050607080910111213.00000CA05B40.02

 VCD  rxFrames  txFrames  Type       ATM Address
   0         0         0  configure  39.020304050607080910111213.00000CA05B43.00
  55         1         4  direct     39.020304050607080910111213.00000CA05B41.02
  56         6         0  distribute 39.020304050607080910111213.00000CA05B41.02
  59         0         1  send       39.020304050607080910111213.00000CA05B42.02
  60         3         0  forward    39.020304050607080910111213.00000CA05B42.02
  84         3         5  data       39.020304050607080910111213.00602F557940.02
```

The following is sample output from the **show lane client** command for a Token Ring LANE:

```
Router# show lane client

LE Client ATM4/0.1  ELAN name: elan1  Admin: up  State: operational
Client ID: 1                LEC up for 2 hours 26 minutes 3 seconds
Join Attempt: 3
HW Address: 0060.4770.4180   Type: token ring           Max Frame Size: 4544
Ring:100    Bridge:2        ELAN Segment ID: 2048
ATM Address: 39.020304050607080910111213.006047704180.01

 VCD  rxFrames  txFrames  Type       ATM Address
   0         0         0  configure  39.020304050607080910111213.006047704183.00
  10         1         3  direct     39.020304050607080910111213.006047704181.01
  11         2         0  distribute 39.020304050607080910111213.006047704181.01
  14         0         0  send       39.020304050607080910111213.006047704182.01
  15         0         0  forward    39.020304050607080910111213.006047704182.01
```

The following is sample output from the **show lane client detail** command.

```
Router# show lane client detail

LE Client ATM1/0.1 ELAN name:xxx Admin:up State:operational
Client ID:2 LEC up for 5 days 40 minutes 45 seconds
ELAN ID:0
This client is running in FSSRP mode.
Join Attempt:14
Known LE Servers:1
Configured Idle Time:5 seconds
Last Fail Reason:Config VC being released
HW Address:00e0.8fcf.d820   Type:ethernet             Max Frame Size:1516

ATM Address:47.009181000000061705B0C01.00E08FCFD820.01
VCDrxFramestxFramesTypeATM Address
0 0 0 configure 47.00918100000000613E5A2F01.006070174823.00

LEC ID:2, State:LESBUS_ACTIVE

52 17783556direct47.00918100000000613E5A2F01.00000C5A0C59.01
5317780distribute47.00918100000000613E5A2F01.00000C5A0C59.01
54 00send47.00918100000000613E5A2F01.00000C5A0C5A.01
55 00forward47.00918100000000613E5A2F01.00000C5A0C5A.01

LEC ID:3, State:LESBUS_ACTIVE
```

```
93122234direct47.00918100000000613E5A2F01.00000ABCD001.09
941220distribute47.00918100000000613E5A2F01.00000ABCD001.09
9700send47.00918100000000613E5A2F01.00000ABCD002.09
0800forward47.00918100000000613E5A2F01.00000ABCD002.09
```

Table 61 describes significant fields shown in the output.

Table 61 show lane client Field Descriptions

Field	Description
LE Client ATM2/0.2	Interface and subinterface of this client.
ELAN name	Name of the ELAN.
Admin	Administrative state, either up or down.
State	Status of this LANE client. Possible states include initialState, lecsConnect, configure, join, busConnect, and operational.
Client ID	The LANE 2-byte client ID assigned by the LANE server.
Join Attempt	The number of attempts made before successfully joining the ELAN.
HW Address	MAC address of this LANE client.
Type	Type of ELAN.
Max Frame Size	Maximum frame size (in bytes) on the ELAN.
Ring	The ring number for the client. This field appears only for Token Ring LANE.
Bridge	The bridge number for the client. This field appears only for Token Ring LANE.
ELAN Segment ID	The ring number for the ELAN. This field appears only for Token Ring LANE.
ATM Address	ATM address of this LANE client.
VCD	Virtual channel descriptor for each of the VCCs established for this LANE client.
rxFrames	Number of frames received.
txFrames	Number of frames sent.
Type	Type of VCC. The Configure Direct VCC is shown in this display as *configure*. The Control Direct VCC is shown as *direct*; the Control Distribute VCC is shown as *distribute*. The Multicast Send VCC and Multicast Forward VC are shown as *send* and *forward*, respectively. The Data Direct VCC is shown as *data*.
ATM Address	ATM address of the LANE component at the other end of this VCC.

Related Commands

Command	Description
lane client	Activates a LANE client on the specified subinterface.
lane fssrp	Enables the special LANE features so that LANE components (such as the LANE configuration server, the LANE client, the LANE server, and the BUS) become aware of FSSRP.

Command	Description
lane server	Activates a LANE server on the specified subinterface.
show lane config	Displays global LANE information for the configuration server configured on an interface.

show lane config

To display global LANE information for the configuration server configured on an interface, use the **show lane config** command in EXEC mode.

AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

show lane config [**interface atm** *slot*/**0**]

ATM Port Adapter on the Cisco 7500 Series Routers

show lane config [**interface atm** *slot*/*port-adapter*/**0**]

Cisco 4500 and 4700 Routers

show lane config [**interface atm** *number*]

Syntax Description

interface atm *slot*/**0**	(Optional) ATM interface slot and port for the following: • AIP on the Cisco 7500 series routers. • ATM port adapter on the Cisco 7200 series routers.
interface atm *slot/port-adapter*/**0**	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
interface atm *number*	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample **show lane config** output for an Ethernet ELAN:

```
Router# show lane config

LE Config Server ATM2/0 config table: cisco_eng
Admin: up  State: operational
LECS Mastership State: active master
list of global LECS addresses (30 seconds to update):
39.020304050607080910111213.00000CA05B43.00  <-------- me
ATM Address of this LECS: 39.020304050607080910111213.00000CA05B43.00 (auto)
 vcd  rxCnt  txCnt  callingParty
  50      2      2  39.020304050607080910111213.00000CA05B41.02 LES elan2 0 active
cumulative total number of unrecognized packets received so far: 0
cumulative total number of config requests received so far: 30
cumulative total number of config failures so far: 12
    cause of last failure: no configuration
    culprit for the last failure: 39.020304050607080910111213.00602F557940.01
```

The following example shows sample **show lane config** output for TR-LANE:

```
Router# show lane config

LE Config Server ATM4/0 config table: eng
Admin: up  State: operational
LECS Mastership State: active master
list of global LECS addresses (40 seconds to update):
39.020304050607080910111213.006047704183.00  <-------- me
ATM Address of this LECS: 39.020304050607080910111213.006047704183.00 (auto)
 vcd  rxCnt  txCnt  callingParty
   7      1      1  39.020304050607080910111213.006047704181.01 LES elan1 0 active
cumulative total number of unrecognized packets received so far: 0
cumulative total number of config requests received so far: 2
cumulative total number of config failures so far: 0
```

Table 62 describes significant fields shown in the output.

Table 62 show lane config Field Descriptions

Field	Description
LE Config Server	Major interface on which the LAN emulated Configuration Server (LECS) is configured.
config table	Name of the database associated with the LECS.
Admin	Administrative state, either up or down.
State	State of the configuration server: down or operational. If down, the reasons field indicates why it is down. The reasons include the following: NO-config-table, NO-nsap-address, and NO-interface-up.
LECS Mastership State	Mastership state of the configuration server. If you have configured simple server redundancy, the configuration server with the lowest index is the active LECS.
list of global LECS addresses	List of LECS addresses.
40 seconds to update	Amount of time until the next update.
<-------- me	ATM address of this configuration server.
ATM Address of this LECS	ATM address of the active configuration server.
auto	Method of ATM address assignment for the configuration server. In this example, the address is assigned by the automatic method.
vcd	Virtual circuit descriptor that uniquely identifies the configure VCC.
rxCnt	Number of packets received.
txCnt	Number of packets sent.
callingParty	ATM NSAP address of the LANE component that is connected to the LECS. “elan1” indicates the ELAN name, “0” indicates the priority number, and “active” indicates that the server is active.

show lane database

To display the database of the configuration server, use the **show lane database** command in EXEC mode.

show lane database [*database-name*]

Syntax Description

database-name	(Optional) Specific database name.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

By default, this command displays the LAN Emulated Configuration Server information displayed by the **show lane config** command.

If no database name is specified, this command shows all databases.

Examples

The following is sample output of the **show lane database** command for an Ethernet LANE:

```
Router# show lane database

LANE Config Server database table 'engandmkt' bound to interface/s: ATM1/0
default elan: none
elan 'eng': restricted
  server 45.000001415555121f.yyyy.zzzz.0800.200c.1001.01 (prio 0) active
  LEC MAC  0800.200c.1100
  LEC NSAP 45.000001415555121f.yyyy.zzzz.0800.200c.1000.01
  LEC NSAP 45.000001415555124f.yyyy.zzzz.0800.200c.1300.01
elan 'mkt':
  server 45.000001415555121f.yyyy.zzzz.0800.200c.1001.02 (prio 0) active
  LEC MAC  0800.200c.1200
  LEC NSAP 45.000001415555121f.yyyy.zzzz.0800.200c.1000.02
  LEC NSAP 45.000001415555124f.yyyy.zzzz.0800.200c.1300.02
```

The following is sample output of the **show lane database** command for a Token Ring LANE:

```
Router# show lane database

LANE Config Server database table 'eng' bound to interface/s: ATM4/0
default elan: elan1
elan 'elan1': un-restricted, local-segment-id 2048
  server 39.020304050607080910111213.006047704181.01 (prio 0) active
```

Table 63 describes significant fields shown in the output.

Table 63 show lane database Field Descriptions

Field	Description
LANE Config Server database	Name of this database and interfaces bound to it.
default elan	Default name, if one is established.
elan	Name of the ELAN whose data is reported in this line and the following indented lines.
un-restricted	Indicates whether this ELAN is restricted or unrestricted.
local-segment-id 2048	Ring number of the ELAN.
server	ATM address of the configuration server.
(prio 0) active	Priority level and simple server redundancy state of this configuration server. If you have configured simple server redundancy, the configuration server with the lowest priority will be active.
LEC MAC	MAC addresses of an individual LANE client in this ELAN. This display includes a separate line for every LANE client in this ELAN.
LEC NSAP	ATM addresses of all LANE clients in this ELAN.

show lane default-atm-addresses

To display the automatically assigned ATM address of each LANE component in a router or on a specified interface or subinterface, use the **show lane default-atm-addresses** command in EXEC mode.

AIP on the Cisco 7500 series routers; ATM port adapter on the Cisco 7200 series

show lane default-atm-addresses [**interface atm** *slot/port.subinterface-number*]

ATM Port Adapter on the Cisco 7500 Series Routers

show lane default-atm-addresses [**interface atm** *slot/port-adapter/port.subinterface-number*]

Cisco 4500 and 4700 Routers

show lane default-atm-addresses [**interface atm** *number.subinterface-number*]

Syntax Description

interface atm *slot/port*	(Optional) ATM interface slot and port for the following: • AIP on the Cisco 7500 series routers. • ATM port adapter on the Cisco 7200 series routers.
interface atm *slot/port-adapter/port*	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
interface atm *number*	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
.subinterface-number	(Optional) Subinterface number.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
11.1	The *number.subinterface-number* argument was added.

Usage Guidelines

It is not necessary to have any of the LANE components running on this router before you use this command.

Examples

The following is sample output of the **show lane default-atm-addresses** command for the ATM interface 1/0 when all the major LANE components are located on that interface:

```
Router# show lane default-atm-addresses interface atm1/0

interface ATM1/0:
```

```
LANE Client:        47.00000000000000000000000.00000C304A98.**
LANE Server:        47.00000000000000000000000.00000C304A99.**
LANE Bus:           47.00000000000000000000000.00000C304A9A.**
LANE Config Server: 47.00000000000000000000000.00000C304A9B.00
note: ** is the subinterface number byte in hex
```

Table 64 describes the significant fields shown in the output.

Table 64 show lane default-atm-addresses Field Descriptions

Field	Description
interface ATM1/0:	Specified interface.
LANE Client:	ATM address of the LANE client on the interface.
LANE Server:	ATM address of the LANE server on the interface.
LANE Bus:	ATM address of the LANE broadcast and unknown server on the interface.
LANE Config Server:	ATM address of the LAN Emulated Configuration Server on the interface.

show lane le-arp

To display the LANE ARP table of the LANE client configured on an interface or any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane le-arp** command in EXEC mode.

AIP on the Cisco 7500 series routers; ATM Port Adapter on the Cisco 7200 series

show lane le-arp [**interface atm** *slot/port*[**.***subinterface-number*] | **name** *elan-name*]

ATM Port Adapter on the Cisco 7500 Series Routers

show lane le-arp [**interface atm** *slot/port-adapter/port*[**.***subinterface-number*] | **name** *elan-name*]

Cisco 4500 and 4700 Routers

show lane le-arp [**interface atm** *number*[**.***subinterface-number*] | **name** *elan-name*]

Syntax Description

interface atm *slot/port*	(Optional) ATM interface slot and port for the following: • AIP on the Cisco 7500 series routers. • ATM port adapter on the Cisco 7200 series routers.
interface atm *slot/port-adapter/port*	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
interface atm *number*	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
.*subinterface-number*	(Optional) Subinterface number.
name *elan-name*	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output of the **show lane le-arp** command for an Ethernet LANE client:

```
Router# show lane le-arp

Hardware Addr   ATM Address                                  VCD  Interface
0000.0c15.a2b5  39.000000000000000000000000.00000C15A2B5.01  39  ATM1/0.1
0000.0c15.f3e5  39.000000000000000000000000.00000C15F3E5.01  25* ATM1/0.1
```

The following is sample output of the **show lane le-arp** command for a Token Ring LANE client:

```
Router# show lane le-arp

Ring Bridge       ATM Address                                     VCD  Interface
512   6           39.020304050607080910111213.00602F557940.01  47  ATM2/0.1
```

Table 65 describes the significant fields shown in the output.

Table 65 show lane le-arp Field Descriptions

Field	Description
Hardware Addr	MAC address, in dotted hexadecimal notation, assigned to the LANE component at the other end of this VCD.
Ring	Route descriptor segment number for the LANE component.
Bridge	Bridge number for the LANE component.
ATM Address	ATM address of the LANE component at the other end of this VCD.
VCD	Virtual circuit descriptor.
Interface	Interface or subinterface used to reach the specified component.

show lane server

To display global information for the LANE server configured on an interface, on any of its subinterfaces, on a specified subinterface, or on an emulated LAN (ELAN), use the **show lane server** command in EXEC mode.

AIP on the Cisco 7500 Series Routers; ATM Port Adapter on the Cisco 7200 Series

show lane server [**interface atm** *slot/port*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

ATM Port Adapter on the Cisco 7500 Series Routers

show lane server [**interface atm** *slot/port-adapter/port*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

Cisco 4500 and 4700 Routers

show lane server [**interface atm** *number*[**.***subinterface-number*] | **name** *elan-name*] [**brief**]

Syntax Description

interface atm *slot/port*	(Optional) ATM interface slot and port for the following: • AIP on the Cisco 7500 series routers. • ATM port adapter on the Cisco 7200 series routers.
interface atm *slot/port-adapter/port*	(Optional) ATM interface slot, port adapter, and port number for the ATM port adapter on the Cisco 7500 series routers.
interface atm *number*	(Optional) ATM interface number for the NPM on the Cisco 4500 or 4700 routers.
.*subinterface-number*	(Optional) Subinterface number.
name *elan-name*	(Optional) Name of the ELAN. The maximum length of the name is 32 characters.
brief	(Optional) Keyword used to display the brief subset of available information.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output from the **show lane server** command for an Ethernet ELAN:

```
Router# show lane server

LE Server ATM2/0.2  ELAN name: elan2  Admin: up  State: operational
type: ethernet         Max Frame Size: 1516
```

```
ATM address: 39.020304050607080910111213.00000CA05B41.02
LECS used: 39.020304050607080910111213.00000CA05B43.00 connected, vcd 51
control distribute: vcd 57, 2 members, 2 packets

proxy/ (ST: Init, Conn, Waiting, Adding, Joined, Operational, Reject, Term)
lecid ST vcd    pkts Hardware Addr  ATM Address
   1  O   54       2 0000.0ca0.5b40 39.020304050607080910111213.00000CA05B40.02
   2  O   81       2 0060.2f55.7940 39.020304050607080910111213.00602F557940.02
```

The following is sample output from the **show lane server** command for a Token Ring ELAN:

```
Router# show lane server

LE Server ATM3/0.1  ELAN name: anubis  Admin: up  State: operational
type: token ring         Max Frame Size: 4544      Segment ID: 2500
ATM address: 47.009181000000000000000000.00000CA01661.01
LECS used: 47.009181000000000000000000.00000CA01663.00 connected, vcd 6
control distribute: vcd 10, 2 members, 4 packets
proxy/ (ST: Init, Conn, Waiting, Adding, Joined, Operational, Reject, Term)
lecid ST vcd    pkts Hardware Addr  ATM Address
   1  O    7       3 400.1         47.009181000000000000000000.00000CA01660.01
                     0000.0ca0.1660 47.009181000000000000000000.00000CA01660.01
   2  O   16       3 300.1         47.009181000000000000000000.00000CA04960.01
                     0000.0ca0.4960 47.009181000000000000000000.00000CA04960.01
```

Table 66 describes the significant fields shown in the output.

Table 66 show lane server Field Descriptions

Field	Description
LE Server ATM2/0.2	Interface and subinterface of this server.
ELAN name	Name of the ELAN.
Admin	Administrative state, either up or down.
State	Status of this LANE server. Possible states for a LANE server include down, waiting_ILMI, waiting_listen, up_not_registered, operational, and terminating.
type	Type of ELAN.
Max Frame Size	Maximum frame size (in bytes) of this type of emulated LAN.
Segment ID	The ring number of the ELAN. This field appears only for Token Ring LANE.
ATM address	ATM address of this LANE server.
LECS used	ATM address of the LANE configuration server being used. This line also shows the current state of the connection between the LANE server and the LAN Emulated Configuration Server (LECS), and the virtual circuit descriptor (VCD) of the circuit connecting them.
control distribute	VCD of the Control Distribute VCC.
proxy	Status of the LANE client at the other end of the Control Distribute VCC.
lecid	Identifier for the LANE client at the other end of the Control Distribute VCC.

Table 66 show lane server Field Descriptions (continued)

Field	Description
ST	Status of the LANE client at the other end of the Control Distribute VCC. Possible states are Init, Conn, Waiting, Adding, Joined, Operational, Reject, and Term.
vcd	Virtual channel descriptor used to reach the LANE client.
pkts	Number of packets sent by the LANE server on the Control Distribute VCC to the LANE client.
Hardware Addr	The top number in this column is the router descriptor, and the second number is the MAC-layer address of the LANE client.
ATM Address	ATM address of the LANE client.

show mls rp

To display MLS details, including specifics for MLSP, use the **show mls rp** command in EXEC mode.

show mls rp [*interface*]

Syntax Description

interface	(Optional) Displays information for one interface. Without this argument, detailed views of all interfaces are displayed.

Command Modes

EXEC

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Examples

The following is sample output for the **show mls rp** command:

```
Router# show mls rp

multilayer switching is globally enabled
mls id is 00e0.fefc.6000
mls ip address 10.20.26.64
mls flow mask is ip-flow
vlan domain name: WBU
   current flow mask: ip-flow
   current sequence number: 80709115
   current/maximum retry count: 0/10
   current domain state: no-change
   current/next global purge: false/false
   current/next purge count: 0/0
   domain uptime: 13:03:19
   keepalive timer expires in 9 seconds
   retry timer not running
   change timer not running
   fcp subblock count = 7

   1 management interface(s) currently defined:
      vlan 1 on Vlan1

   7 mac-vlan(s) configured for multi-layer switching:

      mac 00e0.fefc.6000
         vlan id(s)
         1    10   91   92   93   95   100

   router currently aware of following 1 switch(es):
      switch id 0010.1192.b5ff
```

The following is sample output for the **show mls rp** command for a specific interface:

```
Router# show mls rp int vlan 10

mls active on Vlan10, domain WBU
```

Related Commands

Command	Description
mls rp ip	Enables MLSP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp nde-address	Specifies a NetFlow Data Export address.
mls rp vlan-id	Assigns a VLAN ID.
mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a VTP domain.
show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

show mls rp interface

To display IPX Multilayer Switching (MLS) details for the Route Processor (RP), including specific information about the Multilayer Switching Protocol (MLSP), use the **show mls rp interface** command in privileged EXEC mode.

show mls rp interface *type number*

Syntax Description

type	Interface type.
number	Interface number.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following displays sample output from the **show mls rp interface** command. The interface type is VLAN, and its number is 10.

```
Router# show mls rp interface vlan 10

    IPX MLS active on Vlan 10, domain WBU
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flow(s).
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the route processor.

show mls rp ip multicast

To display hardware-switched multicast flow information about IP multicast Multilayer Switching (MLS), use the **show mls rp ip multicast** command in EXEC mode.

show mls rp ip multicast [**locate**] [*group* [*source*] [*vlan-id*]] | [**statistics**] | [**summary**]

Syntax Description

locate	(Optional) Displays flow information associated with the switch. This keyword applies only to a single router and multiple switches.
group	(Optional) Address of the IP multicast group about which to display information.
source	(Optional) IP multicast source sending to the specified multicast *group* about which to display information.
vlan-id	(Optional) Source VLAN about which to display information.
statistics	(Optional) Displays MLS statistics.
summary	(Optional) Displays MLS summary.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show mls rp ip multicast** command using the **locate** keyword:

```
Router# show mls rp ip multicast locate

Source           Group            Vlan  SwitchIP         SwitchMAC
------           -----            ----  --------         ---------
192.1.10.6       239.255.158.197  10    1.2.10.199       0010.a60b.b4ff
```

The following is sample output of the **show mls rp ip multicast** command for a specific IP multicast group:

```
Router# show mls rp ip multicast 224.1.1.1

Multicast hardware switched flows:
(1.1.13.1, 224.1.1.1) Incoming interface: Vlan13, Packets switched: 61590
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan13

(1.1.9.3, 224.1.1.1) Incoming interface: Vlan9, Packets switched: 0
Hardware switched outgoing interfaces: Vlan20
MFD installed: Vlan9

(1.1.12.1, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 62010
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan12
```

```
(1.1.12.3, 224.1.1.1) Incoming interface: Vlan12, Packets switched: 61980
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan12

(1.1.11.1, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan11

(1.1.11.3, 224.1.1.1) Incoming interface: Vlan11, Packets switched: 62430
Hardware switched outgoing interfaces: Vlan20 Vlan9
MFD installed: Vlan11

Total shortcut installed: 6
```

The following is sample output of the **show mls rp ip multicast** command using the **statistics** keyword:

```
Router# show mls rp ip multicast statistics

MLS Multicast Operation Status:
MLS Multicast configuration and state:
    Router Mac: 0010.298f.0009
    Switch Mac: 0010.0d70.a3ff      Switch IP: 1.2.10.195
    MLS Multicast Operating state: ACTIVE
    Active management vlan: Vlan1, 192.1.4.1
    User configured management vlan: None, 0.0.0.0
    Include-List: IP1 = 192.1.28.2, IP2 = 0.0.0.0
    Router IP used in MLS Multicast messages: 192.1.28.2

MLS Multicast statistics:
    Keepalive sent: 90
    Keepalive ACK received: 90
    Open request sent: 3
    Open request ACK received: 3
    Delete notifications received: 3
    Flow statistics messages received: 181
    Flow message sent: 14
    Flow message Ack received: 14
    Flow message Nack received: 0

    Flow install Ack: 2
    Flow install Nack: 0
    Flow update Ack: 7
    Flow update Nack: 0
    Flow delete Ack: 0
    Complete flow install Ack: 3
    Complete flow install Nack: 0
    Complete flow delete Ack: 1
    Input vlan delete Ack: 0
    Output vlan delete Ack: 0
    Global delete sent: 1

    L2 entry not found error: 0
    LTL entry not found error: 0
    MET entry not found error: 0
    L3 entry not found error: 0
    L3 entry exists error : 0
    Hash collision error : 0
    Sequence number error : 0
    None-supported error : 0
    Generic error : 0
```

The following is sample output of the **show mls rp ip multicast** command using the **summary** keyword:

```
Router# show mls rp ip multicast summary

Switch IP:0.0.0.0  Switch MAC:0000.0000.0000
Number of complete flows: 0
Total hardware-switched flows: 0

Switch IP:1.2.10.199  Switch MAC:0010.a60b.b4ff
Number of complete flows: 1
Total hardware-switched flows: 1
```

Related Commands

Command	Description
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.

show mls rp ipx

To display details for all IPX Multilayer Switching (MLS) interfaces on the IPX MLS router, use the **show mls rp ipx** command in privileged EXEC mode.

show mls rp ipx

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.

Usage Guidelines

This command gives you details about the following:

- MLS status (enabled or disabled) for switch interfaces and subinterfaces
- Flow mask required when creating Layer 3 switching entries for the router
- Current settings for the keepalive timer, retry timer, and retry count
- MLS identifier used in Multilayer Switching Protocol (MLSP) messages
- List of all interfaces in all Virtual Trunk Protocol (VTP) domains enabled for MLS

Examples

The following example displays sample output from the **show mls rp ipx** command for all IPX MLS interfaces on an MLS-RP:

```
Router# show mls rp ipx

    ipx multilayer switching is globally enabled
    ipx mls inbound acl override is globally disabled
    mls id is 0050.73ff.b580
    mls ip address 5.5.5.155
    IPX MLS flow mask is source-destination
    number of domains configured for mls 1

    vlan domain name:Engineering
           current ipx flow mask:source-destination
           ipx current/next global purge:false/false
           ipx current/next purge count:0/0
           current sequence number:4086390283
           current/maximum retry count:0/10
           current domain state:no-change
           domain uptime:03:13:09
           keepalive timer expires in 3 seconds
           retry timer not running
           change timer not running

       1 management interface(s) currently defined:
              vlan 21 on Vlan21
```

```
2 mac-vlan(s) enabled for ipx multi-layer switching:

       mac 0010.0738.2917
          vlan id(s)
          22

       mac 0050.73ff.b5b8
          vlan id(s)
          21

router currently aware of following 1 switch(es):
       switch id 00e0.fe4a.aeff
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

show mls rp vtp-domain

To display IPX Multilayer Switching (MLS) interfaces for a specific Virtual Trunk Protocol (VTP) domain on the Route Processor (RP), use the **show mls rp vtp-domain** command in privileged EXEC mode.

show mls rp vtp-domain *domain-name*

Syntax Description

domain-name	The name of the VTP domain whose MLS interfaces will be displayed.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Examples

This example shows details about IPX MLS interfaces in a VTP domain named WBU:

```
Router# show mls rp vtp-domain WBU

    vlan domain name: WBU
    current ipx flow mask: destination
           ipx current/next global purge: false/false
           ipx current/next purge count: 0/0
           current ipx flow mask: destination
           ipx current/next global purge: false/false
           ipx current/next purge count: 0/0
           current sequence number: 590678296
           current/maximum retry count: 0/10
           current domain state: no-change
           domain uptime: 1d14h
           keepalive timer expires in 3 seconds
           retry timer not running
           change timer not running
           fcp subblock count = 20

       1 management interface(s) currently defined:
              vlan 2 on Vlan2

       20 mac-vlan(s) configured for multi-layer switching

       17 mac-vlan(s) enabled for ipx multi-layer switching:

              mac 0010.0738.2917
                 vlan id(s)
         2    3    4    5    6    7    8    9    10   12   13
         14   15   88   99

              mac 0090.6dfc.5800
```

```
          vlan id(s)
          20   21

18 mac-vlan(s) enabled for ipx multi-layer switching:

       mac 0010.0738.2917
          vlan id(s)
          2    3    4    5    6    7    8    9    10   11   12
          13   14   15   66   77   88   99

router currently aware of following 1 switch(es):
       switch id 0010.141f.6fff
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.

show mpls forwarding-table

To display the contents of the MPLS forwarding information base (LFIB), use the **show mpls forwarding-table** user EXEC command.

show mpls forwarding-table [{*network* {*mask* | *length*} | **labels** *label* [**-** *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]

Syntax Description

network	(Optional) Destination network number.
mask	(Optional) IP address of the destination mask whose entry is to be shown.
length	(Optional) Number of bits in mask of 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 *tunnel-id*	(Optional) Displays only entries with the specified LSP tunnel, or all LSP tunnel entries.
detail	(Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit (MTU), and all labels).

Command Modes

User EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.
12.1(3)T	This command was modified to reflect new MPLS IETF terminology and CLI command syntax.

Usage Guidelines

The optional parameters described allow specification of a subset of the entire LFIB.

Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes tag Outgoing       Next Hop
tag   tag or VC     or Tunnel Id      switched  interface
26    Untagged      10.253.0.0/16     0         Et4/0/0        172.27.32.4
28    1/33          10.15.0.0/16      0         AT0/0.1        point2point
29    Pop tag       10.91.0.0/16      0         Hs5/0          point2point
      1/36          10.91.0.0/16      0         AT0/0.1        point2point
30    32            10.250.0.97/32    0         Et4/0/2        10.92.0.7
      32            10.250.0.97/32    0         Hs5/0          point2point
34    26            10.77.0.0/24      0         Et4/0/2        10.92.0.7
      26            10.77.0.0/24      0         Hs5/0          point2point
35    Untagged  [T] 10.100.100.101/32 0         Tu301          point2point
36    Pop tag       168.1.0.0/16      0         Hs5/0          point2point
```

```
      1/37          168.1.0.0/16      0         AT0/0.1       point2point

[T]     Forwarding through a TSP tunnel.
        View additional tagging info with the 'detail' option
```

The following is 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 tag Outgoing       Next Hop
tag   tag or VC     or Tunnel Id      switched  interface
26    Untagged      10.253.0.0/16     0         Et4/0/0        172.27.32.4
        MAC/Encaps=0/0, MTU=1504, Tag Stack{}
28    1/33          10.15.0.0/16      0         AT0/0.1        point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{1/33(vcd=2)}
        00020900 00002000
29    Pop tag       10.91.0.0/16      0         Hs5/0          point2point
        MAC/Encaps=4/4, MTU=4474, Tag Stack{}
        FF030081
      1/36          10.91.0.0/16      0         AT0/0.1        point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{1/36(vcd=3)}
        00030900 00003000
30    32            10.250.0.97/32    0         Et4/0/2        10.92.0.7
        MAC/Encaps=14/18, MTU=1500, Tag Stack{32}
        006009859F2A00E0F7E984828847 00020000
      32            10.250.0.97/32    0         Hs5/0          point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{32}
        FF030081 00020000
34    26            10.77.0.0/24      0         Et4/0/2        10.92.0.7
        MAC/Encaps=14/18, MTU=1500, Tag Stack{26}
        006009859F2A00E0F7E984828847 0001A000
      26            10.77.0.0/24      0         Hs5/0          point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{26}
        FF030081 0001A000
35    Untagged      10.100.100.101/32 0         Tu301          point2point
        MAC/Encaps=0/0, MTU=1504, Tag Stack{}, via Et4/0/2
36    Pop tag       168.1.0.0/16      0         Hs5/0          point2point
        MAC/Encaps=4/4, MTU=4474, Tag Stack{}
        FF030081
      1/37          168.1.0.0/16      0         AT0/0.1        point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{1/37(vcd=4)}
        00040900 00004000
```

Table 67 describes the significant fields shown in the output.

Table 67 show mpls forwarding-table Field Descriptions

Field	Description
Local tag	Label assigned by this router.
Outgoing tag or VC	Label assigned by the next hop, or VPI/VCI used to get to next hop. The entries that you can specify in this column include the following: • [T]—Means forwarding through a TSP tunnel. • "Untagged"—Means there is no label for the destination from the next hop, or label switching is not enabled on the outgoing interface. • "Pop tag"—Means that the next hop advertised an implicit NULL label for the destination, and that this router popped the top label.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are going.

Table 67 show mpls forwarding-table Field Descriptions (continued)

Field	Description
Bytes tag switched	Number of bytes switched with this incoming label.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.
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	Maximum transmission unit (MTU) of the labeled packet.
Tag Stack	All the outgoing labels. If the outgoing interface is TC-ATM, the VCD is also shown.
00020900 00002000	The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header.

show mpls interfaces

To display information about one or more interfaces that have been configured for label switching, use the **show mpls interfaces** privileged EXEC command.

show mpls interfaces [*interface*] [**detail**]

show mpls interfaces [**all**]

Syntax Description

interface	(Optional) Defines the interface about which to display label switching information.
detail	(Optional) Displays detailed label switching information for the specified interface.
all	(Optional) When the **all** keyword is specified in the absence of other optional parameters, the command displays LDP discovery information for all VPNs.

Defaults

If no optional keyword or parameter is specified in this command, summary information is displayed for each interface that has been configured for label switching.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.
12.1(3)T	This command was modified to reflect new MPLS IETF terminology and CLI command syntax.

Usage Guidelines

This command shows MPLS information about the specified interface, or about all of the interfaces for which MPLS has been configured.

Examples

The following is sample output generated by 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
```

Note If an interface uses LC-ATM procedures, the associated line in the display is flagged with the following notation "(`ATM labels`)".

Table 68 describes the significant fields in the output.

Table 68 show mpls interfaces Field Descriptions

Field	Description
Interface	Interface name.
IP	"Yes" if IP label switching (sometimes called hop-by-hop label switching) has been enabled on this interface.
Tunnel	"Yes" if LSP tunnel labeling has been enabled on this interface.
Operational	Operational state. "Yes" if packets are being labeled.
MTU	Maximum number of data bytes per labeled packet that will be transmitted.

The following is sample output from the **show mpls interfaces** command when you specify 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
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables label switching of IPv4 packets on all interfaces.
mpls ip (interface configuration)	Enables label switching of IPv4 packets on the associated interface.

Command	Description
mpls traffic-eng tunnels (global configuration)	Enables MPLS traffic engineering tunnel signalling on a device.
mpls traffic-eng tunnels (interface configuration)	Enables MPLS traffic engineering tunnel signalling on an interface.

show mpls label range

To display the range of local labels available for use on packet interfaces, use the **show mpls label range** privileged EXEC command.

show mpls label range

Syntax Description

This command has no optional keywords or arguments

Defaults

This command has no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(9)ST	This command was introduced.

Usage Guidelines

You can use the **mpls label range** command to configure a range for local labels that is different from the default range. If the newly configured range does not overlap the current range, then the new range will not take effect until the router is reloaded. In this situation, 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
% Label range changes will take effect at the next reload.
Router(config)# exit

Router# show mpls label range

Downstream label pool: Min/Max label: 16/100000
   [Configured range for next reload: Min/Max label: 200/120000]
```

Related Commands

Command	Description
mpls label range	Configures a range of values for use as local labels.

show mpls traffic-eng autoroute

To show tunnels that are announced to the Interior Gateway Protocol (IGP), including interface, destination, and bandwidth, use the **show mpls traffic-eng autoroute** EXEC command.

show mpls traffic-eng autoroute

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

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 2.2.2.2, absolute metric 11)
    Tunnel1022 (traffic share 3333, nexthop 2.2.2.2, relative metric -3)
  destination 0003.0003.0003.00 has 2 tunnels
    Tunnel1032 (traffic share 10000, nexthop 3.3.3.3)
    Tunnel1031 (traffic share 10000, nexthop 3.3.3.3, relative metric -1)
```

Table 69 describes the significant fields shown in the output.

Table 69 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.

Table 69 show mpls traffic-eng autoroute Field Descriptions (continued)

Field	Description
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 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** EXEC command.

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.

Defaults

No default behavior or values.

Command Modes

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.

Examples

The following is sample output from the **show mpls traffic-eng link-management admission-control** command:

```
Router2# 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 70 describes the significant fields shown in the output.

Table 70 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.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.

Table 70 show mpls traffic-eng link-management admission-control Field Descriptions (continued)

Field	Description
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 show local link information that MPLS traffic engineering link management is currently flooding into the global traffic engineering topology, use the **show mpls traffic-eng link-management advertisements** EXEC command.

show mpls traffic-eng link-management advertisements

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.

Examples

The following is sample output from the **show mpls traffic-eng link-management advertisements** command:

```
Router1# 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 71 describes the significant fields shown in the output.

Table 71 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 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 on this link.
Reservable Bandwidth	Amount of bandwidth that is available for reservation.
Attribute Flags	Attribute flags of the link are being flooded.

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 show current local link information, use the **show mpls traffic-eng link-management bandwidth-allocation** EXEC command.

show mpls traffic-eng link-management bandwidth-allocation [*interface-name*]

Syntax Description

interface-name	(Optional) Displays only tunnels that were admitted on the specified interface.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.

Usage Guidelines

Advertised information might differ from the current information, depending on how flooding was configured.

Examples

The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation** command:

```
Router1# 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 72 describes the significant fields shown in the output.

Table 72 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.

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** EXEC command.

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.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

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: 0.0.0.0)
Link ID::  PO1/0/0
    Neighbor ID:  0000.0026.0001.00 (area: isis level-1, IP: 170.1.1.2)
```

Table 73 describes the significant fields shown in the output.

Table 73 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 show interface resource and configuration information, use the **show mpls traffic-eng link-management interfaces** EXEC command.

show mpls traffic-eng link-management interfaces [*interface-name*]

Syntax Description

interface-name	(Optional) Displays information only for the specified interface.

Defaults

Displays resource and configuration information for all configured interfaces.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.

Examples

The following is sample output from the **show mpls traffic-eng link-management interfaces** command:

```
Router1# 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 0.0.0.0 (Up)
    Flooding Status for each configured area [1]:
      IGP Area[1]: isis level-1: flooded
```

Table 74 describes the significant fields shown in the output.

Table 74 show mpls traffic-eng link management interfaces Field Descriptions

Field	Description
Links Count	Number of links that were enabled for use with MPLS traffic engineering.
Link ID	Index of the link.
Physical Bandwidth	Link's bandwidth capacity (in kBps).

Table 74 show mpls traffic-eng link management interfaces Field Descriptions (continued)

Field	Description
Max Reservable BW	Amount of reservable bandwidth on this link.
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 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 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 summary	Displays a summary of link management information.

show mpls traffic-eng link-management summary

To show a summary of link management information, use the **show mpls traffic-eng link-management summary** EXEC command.

show mpls traffic-eng link-management summary [*interface-name*]

Syntax Description

interface-name	(Optional) Displays information only for the specified interface.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.

Examples

The following is sample output from the **show mpls traffic-eng link-management summary** command:

```
Router1# 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 75 describes the significant fields shown in the output.

Table 75 show mpls traffic-eng link-management summary Field Descriptions

Field	Description
Links Count	Number of links configured for 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 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.

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 topology

To show the MPLS traffic engineering global topology currently known at this node, use the **show mpls traffic-eng topology** EXEC command.

show mpls traffic-eng topology [{*A.B.C.D* | **igp-id** {**isis** *nsapaddr* | **ospf** *A.B.C.D*}] [**brief**]

Syntax Description

A.B.C.D	(Optional) Node IP address (router identifier to interface address).
igp-id	(Optional) Node IGP router identifier.
isis *nsapaddr*	(Optional) Node router identification, if IS-IS is enabled.
ospf *A.B.C.D*	(Optional) Node router identifier, if OSPF is enabled.
brief	(Optional) Brief form of the output; gives a less detailed version of the topology.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.

Examples

The following is sample output from the **show mpls traffic-eng topology** command:

```
Router1# show mpls traffic-eng topology 10.106.0.6

IGP Id:0001.0000.0001.00, MPLS TE Id:10.106.0.6 Router Node  id 1
      link[0 ]:Nbr IGP Id:0001.0000.0001.02, nbr_node_id:3, gen:14
          frag_id 0, Intf Address:10.1.0.6
          admin_weight:10, attribute_flags:0x0
          physical_bw:10000 (kbps), max_reservable_bw:5000 (kbps)
               allocated_bw   reservable_bw      allocated_bw   reservable_bw
               ------------   -------------      ------------   -------------
         bw[0]:0              5000         bw[1]:3000           2000
         bw[2]:0              2000         bw[3]:0              2000
         bw[4]:0              2000         bw[5]:0              2000
         bw[6]:0              2000         bw[7]:0              2000
```

Table 76 describes the significant fields shown in the output.

Table 76 show mpls traffic-eng topology Field Descriptions

Field	Description
IGP Id	Identification of the advertising router.
MPLS TE Id	MPLS traffic engineering node identifier.

Table 76 show mpls traffic-eng topology Field Descriptions (continued)

Field	Description
Nbr IGP Id	Neighbor IGP interface.
nbr_node_id	Neighbor IGP router identifier.
gen	Generation number of the link-state packet. This internal number is incremented when any new link-state packet is received.
frag_id	IGP LSA fragment identifier.
Intf Address	This link's interface address.
admin_weight	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 that you can reserve on a link.
allocated_bw	Amount of bandwidth allocated at that priority.
reservable_bw	Amount of available bandwidth reservable at that priority.

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** EXEC command.

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.

Defaults

The specified constraints override any constraints obtained from a reference tunnel.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following is sample output from the **show mpls traffic-eng topology path** command:

```
Router1# 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
Router1#
```

Table 77 describes the significant fields shown in the output.

Table 77 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 show information about tunnels, use the **show mpls traffic-eng tunnels** EXEC command.

show mpls traffic-eng tunnels *tunnel-interface* [**brief**]

show mpls traffic-eng tunnels
[**destination** *address*]
[**source-id** {*num* | *ipaddress* | *ipaddress num*}]
[**role** {**all** | **head** | **middle** | **tail** | **remote**}]
[{**up** | **down**}]
[**name** *string*]
[**suboptimal constraints** {**none** | **current** | **max**}]
[{[**interface in** *phys-intf*] [**interface out** *phys-intf*] | [**interface** *phys-intf*]}]
[**brief**]

Syntax Description

tunnel-interface	Displays information for the specified tunneling interface.
brief	(Optional) Displays the information in brief format.
destination *address*	(Optional) Restricts the display to tunnels destined to the specified IP address.
source-id	(Optional) Restricts the display to tunnels with a matching source IP address or tunnel number.
num	(Optional) Tunnel number.
ipaddress	(Optional) Source IP address.
ipaddress num	(Optional) Source IP address and tunnel number.
role	(Optional) Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
all	(Optional) Displays all tunnels.
head	(Optional) Displays tunnels with their heads at this router.
middle	(Optional) Displays tunnels with their midpoints at this router.
tail	(Optional) Displays tunnels with their tails at this router.
remote	(Optional) Displays tunnels with their heads at another router; this is a combination of the **middle** and **tail** keyword values.
up	(Optional) Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
down	(Optional) Displays tunnels that are down.
name *string*	(Optional) Displays tunnels with the specified name. The tunnel name is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel name is included in the signalling message so it is available at all hops.
suboptimal constraints none	(Optional) Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the IGP's shortest path.
suboptimal constraints current	(Optional) 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.

suboptimal constraints max	(Optional) Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options, and considering only the network's capacity. Selected tunnels would have a shorter path if no other tunnels were consuming network resources.
interface in *phys-intf*	(Optional) Displays tunnels that use the specified input interface.
interface out *phys-intf*	(Optional) Displays tunnels that use the specified output interface.
interface *phys-intf*	(Optional) Displays tunnels that use the specified interface as an input or output interface.
brief	(Optional) Specifies one line per tunnel.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The new **brief** format includes input and output interface information. The **suboptimal** and **interface** keywords were added to the nonbrief format. The nonbrief, nonsummary formats each include the history of LSP selection.

Examples

The following is sample output from the **show mpls traffic-eng tunnels brief** command:

```
Router1# 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
Router1_t1                       10.112.0.12      -          Et4/0/1    up/up
tagsw-r11_t2                     10.112.0.12      -          unknown    up/down
tagsw-r11_t3                     10.112.0.12      -          unknown    admin-down
tagsw-r11_t1000                  10.110.0.10      -          unknown    up/down
tagsw-r11_t2000                  10.110.0.10      -          Et4/0/1    up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Table 78 describes the significant fields shown in the output.

Table 78 show mpls traffic-eng tunnels Field Descriptions

Field	Description
LSP Tunnels Process	Status of the LSP tunnels process.
RSVP Process	Status of the RSVP process.
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Schedule for periodic reoptimization.

Table 78 show mpls traffic-eng tunnels Field Descriptions (continued)

Field	Description
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, admin-down or up. For nonheads, signalled.

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 signalling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signalling on an interface.

show mpls traffic-eng tunnels summary

To show summary information about tunnels, use the **show mpls traffic-eng tunnels summary** EXEC command.

show mpls traffic-eng tunnels summary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

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
    RSVP Process:                   running
    Forwarding:                     enabled
    Head: 1 interfaces, 1 active signalling attempts, 1 established
          1 activations, 0 deactivations
    Midpoints: 0, Tails: 0
    Periodic reoptimization:        every 3600 seconds, next in 3436 seconds
```

Table 79 describes the significant fields shown in the output.

Table 79 show mpls traffic-eng tunnels summary Field Descriptions

Field	Description
LSP Tunnels Process	MPLS traffic engineering has or has not been enabled.
RSVP Process	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 CEF switching.)
Head	Summary information about tunnel heads at this device.
Interfaces	Number of MPLS traffic engineering tunnel interfaces.
Active signalling attempts	LSPs currently successfully signalled or being signalled.
Established	LSPs currently signalled.
activations	Signalling attempts initiated.

Table 79 show mpls traffic-eng tunnels summary Field Descriptions (continued)

Field	Description
deactivations	Signalling attempts terminated.
Periodic reoptimization	Frequency of periodic reoptimization and time until the next periodic reoptimization.

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 signalling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signalling on an interface.

show mpoa client

To display a summary of information regarding one or all MPCs, use the **show mpoa client** command in EXEC mode.

show mpoa client [**name** *mpc-name*] [**brief**]

Syntax Description

name *mpc-name*	(Optional) Name of the MPC with the specified name.
brief	(Optional) Output limit of the command.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

If you omit the **name** keyword, the command displays information for all MPCs.

Examples

The following is sample output from the **show mpoa client** command:

```
Router# show mpoa client name ip_mpc brief

MPC Name: ip_mpc, Interface: ATM1/0, State: Up
MPC actual operating address: 47.00918100000000613E5A2F01.0010A6943825.00
Shortcut-Setup Count: 1, Shortcut-Setup Time: 1
Lane clients bound to MPC ip_mpc: ATM1/0.1
Discovered MPS neighbours                    kp-alv   vcd     rxPkts     txPkts
47.00918100000000613E5A2F01.006070174824.00     59    30         28          2
Remote Devices known                                  vcd     rxPkts     txPkts
47.00918100000000613E5A2F01.00000C5A0C5D.00            35          0         10
```

Table 80 describes the significant fields shown in the output.

Table 80 show mpoa client Field Descriptions

Field	Description
MPC Name	Name specified for the MPC.
Interface	Interface to which the MPC is attached.
State	Current state of the MPC.
MPC actual operating address	ATM address of the MPC.
Shortcut-Setup Count	Current number specified by the **shortcut-frame-count** command.
Shortcut-Setup Time	Current value specified by the **shortcut-frame-time** command.
Lane clients bound to MPC ip_mpc	List of LANE clients currently bound to MPC ip_mpc.

Table 80 show mpoa client Field Descriptions (continued)

Field	Description
Discovered MPS neighbours	List of learned MPS addresses.
kp-alv	Number of seconds until the next keepalive message should be received.
vcd	Number that identifies the virtual circuit.
rxPkts	Number of packets received from the learned MPS.
txPkts	Number of packets sent to the learned MPS.
Remote Devices known	List of other devices (typically other MPCs) not in this ELAN.
vcd	Number that identifies the virtual circuit to that MPC.
rxPkts	Number of packets received from the learned remote device.
txPkts	Number of packets sent to the learned remote device.

Related Commands

Command	Description
clear mpoa client name	Clears the ingress and egress cache entries.

show mpoa client cache

To display the ingress or egress cache entries matching the IP addresses for the MPCs, use the **show mpoa client cache** command in EXEC mode.

show mpoa client [**name** *mpc-name*] **cache** [**ingress** | **egress**] [**ip-address** *ip-address*]

Syntax Description

name *mpc-name*	(Optional) Name of the MPC with the specified name.
ingress	(Optional) Displays ingress cache entries associated with an MPC.
egress	(Optional) Displays egress cache entries associated with an MPC.
ip-address *ip-address*	(Optional) Displays cache entries that match the specified IP address.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Examples

The following is sample output from the **show mpoa client cache** command for a specific MPC:

```
Router# show mpoa client ip_mpc cache

MPC Name: ip-mpc, Interface: ATM1/0, State: Up
MPC actual operating address: 47.00918100000000613E5A2F01.0010A6943825.00
Shortcut-Setup Count: 1, Shortcut-Setup Time: 1
Number of Ingress cache entries: 1
MPC Ingress Cache Information:
Dst IP addr     State   vcd Expires Egress MPC Atm address
20.20.20.1      RSVLD    35   11:38 47.00918100000000613E5A2F01.00000C5A0C5D.00
Number of Egress cache entries: 1
MPC Egress Cache Information:
Dst IP addr         Dst MAC       Src MAC     MPSid  Elan Expires  CacheId  Tag
10.10.10.1      0000.0c5a.0c58 0060.7017.4820     9     2   11:55        1    1
```

Table 81 describes the significant fields shown in the output.

Table 81 show mpoa client cache Field Descriptions

Field	Description
MPC Name	Name specified for the MPC.
Interface	Interface to which the MPC is attached.
State	Current state of the MPC (up or down).
MPC actual operating address	ATM address of the MPC.
Shortcut-Setup Count	Current number specified by the **shortcut-frame-count** command.
Number of Ingress cache entries	Number of entries in the ingress cache.

Table 81 show mpoa client cache Field Descriptions (continued)

Field	Description
MPC Ingress Cache Information	
Dst IP addr	IP address of the destination.
State	State of the ingress cache entry. (Valid states are initialized, trigger, refresh, hold_down, resolved, and suspended..)
vcd	Number that identifies the virtual circuit.
Expires	Time in minutes or seconds until the ingress cache entry expires.
Egress MPC Atm address	ATM address of the egress MPC.
Number of Egress cache entries	Number of entries in the egress cache.
MPC Egress Cache Information	
Dst IP addr	IP address of the destination.
Dst MAC	MAC address of the destination.
Src MAC	MAC address of the source.
MPSid	Unique number representing the egress MPS.
Elan	ELAN identifier of the ELAN serving this destination IP address.
Expires	Time in minutes or seconds until the egress cache entry expires.
CacheID	Cache identifier.
Tag	Label (tag) identifier.

show mpoa client statistics

To display all the statistics collected by an MPC, use the **show mpoa client statistics** command in EXEC mode.

show mpoa client [**name** *mpc-name*] **statistics**

Syntax Description

name *mpc-name*	(Optional) Specifies the name of the MPC.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

This command displays all the statistics collected by an MPC.

Examples

The following is sample output from the **show mpoa client statistics** command for the MPC named ip_mpc:

```
Router# show mpoa client name ip_mpc statistics

MPC Name: ip_mpc, Interface: ATM1/0, State: Up
MPC actual operating address: 47.00918100000000613E5A2F01.0010A6943825.00
Shortcut-Setup Count: 1, Shortcut-Setup Time: 1

                            Transmitted       Received
MPOA Resolution Requests              2              0
MPOA Resolution Replies               0              2
MPOA Cache Imposition Requests        0              0
MPOA Cache Imposition Replies         0              0
MPOA Cache Purge Requests             0              0
MPOA Cache Purge Replies              0              0
MPOA Trigger Request                  0              0
NHRP Purge Requests                   0              0


Invalid MPOA Data Packets Received: 0
```

show mpoa default-atm-addresses

To display the default ATM addresses for the MPC, use the **show mpoa default-atm-addresses** command in EXEC mode.

show mpoa default-atm-addresses

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Examples

The following is sample output from the **show mpoa default-atm-addresses** command when the switch prefix is NOT available:

```
Router# show mpoa default-atm-addresses

interface ATM1/0:
MPOA Server: ...006070174824.**
MPOA Client: ...006070174825.**
note: ** is the MPS/MPC instance number in hex

interface ATM2/0:
MPOA Server: ...006070174844.**
MPOA Client: ...006070174845.**
note: ** is the MPS/MPC instance number in hex
```

The following is sample output from the **show mpoa default-atm-addresses** command when the switch prefix is available:

```
Router# show mpoa default-atm-addresses

interface ATM1/0:
MPOA Server: 47.0091810000000613E5A2F01.006070174824.**
MPOA Client: 47.0091810000000613E5A2F01.006070174825.**
note: ** is the MPS/MPC instance number in hex

interface ATM2/0:
MPOA Server: 47.10000000000000000000000.006070174844.**
MPOA Client: 47.10000000000000000000000.006070174845.**
note: ** is the MPS/MPC instance number in hex
```

Table 82 describes the significant fields shown in the output.

Table 82 show mpoa default-atm-addresses Field Descriptions

Field	Description
interface ATM1/0	Specified interface.
MPOA Server	ATM address of the MPOA server on the interface.
MPOA Client	ATM address of the MPOA client on the interface.

show mpoa server

To display information about any specified MPS or all MPSs in the system, depending on whether the name of the required MPS is specified, use the **show mpoa server** command in EXEC mode.

show mpoa server [**name** *mps-name*]

Syntax Description

name *mps-name*	(Optional) Specifies the name of the MPOA server.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)WA4(5)	This command was introduced.

Usage Guidelines

The command displays information about server configuration parameters. It also displays information about LAN Emulated Clients (LECs) that are bound to the MPOA server neighbors (both MPC and MPS).

Examples

The following is sample output from the **show mpoa server** command, with a specified name:

```
Router# show mpoa server name ip_mps

MPS Name: ip_mps, MPS id: 0, Interface: ATM1/0, State: up
network-id: 1, Keepalive: 25 secs, Holding time: 1200 secs
Keepalive lifetime: 75 secs, Giveup time: 40 secs
MPS actual operating address: 47.00918100000000613E5A2F01.006070174824.00
Lane clients bound to MPS ip_mps: ATM1/0.1 ATM1/0.2
Discovered neighbours:
MPC 47.00918100000000613E5A2F01.00000C5A0C5D.00 vcds: 39(R,A)
MPC 47.00918100000000613E5A2F01.0010A6943825.00 vcds: 40(R,A)
```

Table 83 describes the significant fields shown in the output.

Table 83 show mpoa server Field Descriptions

Field	Description
MPS Name	Name of the MPOA server.
MPS id	ID of the MPOA server.
Interface	Interface to which the MPS is attached.
State	State of the MPOA server: up or down.
network-id	Network ID used for partitioning.
Keepalive	Keepalive time value.
Holding time	Holding time value.
Keepalive lifetime	Keepalive lifetime value.

Table 83 show mpoa server Field Descriptions (continued)

Field	Description
Giveup time	Minimum time to wait before giving up on a pending resolution request.
MPS actual operating address	Actual control address of this MPS.
Lane clients bound to MPS ip_mps	List of LANE clients served by the MPS.
Discovered neighbours	MPOA devices discovered by the clients bound to this MPS.

Related Commands

Command	Description
clear mpoa server name	Clears the ingress and egress cache entries of one or all MPCs.

show mpoa server cache

To display ingress and egress cache entries associated with an MPS, use the **show mpoa server cache** command in EXEC mode.

show mpoa server [**name** *mps-name*] **cache** [**ingress** | **egress**] [**ip-address** *ip-address*]

Syntax Description

name *mps-name*	(Optional) Specifies the name of an MPOA server.
ingress	(Optional) Displays ingress cache entries associated with a server.
egress	(Optional) Displays egress cache entries associated with a server.
ip-address *ip-address*	(Optional) Displays the entries that match the specified IP address.

Command Modes

EXEC

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command displays ingress and egress cache entries associated with an MPS.

Examples

The following is sample output from the **show mpoa server cache** command, with a name specified:

```
Router# show mpoa server name ip_mps cache

MPS Name: ip_mps, MPS id: 0, Interface: ATM1/0, State: up
network-id: 1, Keepalive: 25 secs, Holding time: 1200 secs
Keepalive lifetime: 75 secs, Giveup time: 40 secs
MPS actual operating address: 47.00918100000000613E5A2F01.006070174824.00
Number of Ingress cache entries: 1
Ingress Cache information:
  IP address      Ingress MPC ATM Address                       Remaining Time
  20.20.20.1      47.00918100000000613E5A2F01.0010A6943825.00   19:07
Number of Egress cache entries: 1
Egress Cache information:
  Dst IP address  Ingress MPC ATM Address                       Remaining Time
  20.20.20.1      47.00918100000000613E5A2F01.0010A6943825.00   19:06
  src IP 20.20.20.2, cache Id 1
```

Table 84 describes the significant fields shown in the output.

Table 84 show mpoa server cache Field Descriptions

Field	Description
MPS Name	Name of the MPOA server.
MPS id	ID of the MPOA server.
Interface	Interface to which the MPS is attached.

Table 84 show mpoa server cache Field Descriptions (continued)

Field	Description
State	State of the MPOA server: up or down.
network-id	Network ID used for partitioning.
Keepalive	Keepalive time value.
Holding time	Holding time value.
Keepalive lifetime	Keepalive lifetime value.
Giveup time	Minimum time to wait before giving up on a pending resolution request.
MPS actual operating address	Actual control address of this MPS.
Number of Ingress cache entries	Number of entries in the ingress cache.
Ingress Cache information	Information of ingress cache.
IP address	IP address of the MPC.
Ingress MPC ATM Address	ATM address of the ingress MPC.
Remaining Time	Time for which the cache entry is valid.
Number of Egress cache entries	Number of entries in the egress cache.
Egress Cache information	Information of egress cache.
Dst IP address	IP address of the destination.
src IP	IP address of the source MPS that originated the NHRP resolution request.
cache Id	Cache identifier.

show mpoa server statistics

To display all the statistics collected by an MPS, use the **show mpoa server statistics** command in EXEC mode.

show mpoa server [**name** *mps-name*] **statistics**

Syntax Description

name *mps-name*	(Optional) Specifies the name of an MPOA server.

Command Modes

EXEC

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command will display all the statistics collected by an MPS. The statistics pertain to the ingress or egress cache entry creation, deletion, and failures.

Examples

The following is a sample output from the **show mpoa server statistics** command, with a name specified:

```
Router# show mpoa server name ip_mps statistics

MPS Name: ip_mps, MPS id: 0, Interface: ATM1/0, State: up
network-id: 1, Keepalive: 25 secs, Holding time: 1200 secs
Keepalive lifetime: 75 secs, Giveup time: 40 secs
MPS actual operating address: 47.00918100000000613E5A2F01.006070174824.00
Opcode                            Transmitted    Received
------------------------------------------------------------
MPOA Resolution Requests                             2
MPOA Resolution Replies                      2
MPOA Cache Imposition Requests               1
MPOA Cache Imposition Replies                        1
MPOA Egress Cache Purge Requests                     0
MPOA Egress Cache Purge Replies              0
NHRP Resolution Requests                     0       0
NHRP Resolution Replies                      0       0
NHRP Purge Requests                          0       0
```

Table 85 describes the significant fields shown in the output.

Table 85 show mpoa server statistics Field Descriptions

Field	Description
MPS Name	Name of the MPOA server.
MPS id	ID of the MPOA server.
Interface	Specified interface.

Table 85 show mpoa server statistics Field Descriptions (continued)

Field	Description
State	State of the MPOA server: up or down.
network-id	Network ID used for partitioning.
Keepalive	Keepalive time value.
Holding time	Holding time value.
Keepalive lifetime	Keepalive lifetime value.
Giveup time	Minimum time to wait before giving up on a pending resolution request.
MPS actual operating address	Actual control address of this MPS.

show pxf accounting

To show PXF switching statistics for individual interfaces, use the **show pxf accounting** EXEC command.

show pxf accounting *interface* [*slot/port*]

Syntax Description

interface	Specifies the type of interface to display.
slot	(Optional) Backplane slot number. On the Cisco 7200 VXR series routers, the value can be from 0 to 6.
port	(Optional) Port number of the interface. On the Cisco 7200 VXR series routers, the value can be from 0 to 5.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

You can display information about the following interface types using the **show pxf accounting** command, as shown in Table 86:

Table 86 show pxf accounting Interface Types

Keyword	Interface Type
atm	ATM interface.
ethernet	Ethernet interface.
fastethernet	FastEthernet interface.
hssi	High Speed Serial interface.
null	Null interface.
pos	Packet-over-SONET interface.
serial	Synchronous serial interface.
summary	PXF summary statistics.

The following is sample output from the **show pxf accounting ?** command:

```
Router# show pxf accounting ?

  ATM           ATM interface
```

```
  Ethernet      IEEE 802.3
  FastEthernet  FastEthernet IEEE 802.3
  Hssi          High Speed Seriel Interface
  Null          Null interface
  POS           Packet over Sonet
  Serial        Serial
  summary       PXF summary statistics
```

The following is sample output from the **show pxf accounting** *ethernet* command using an Ethernet interface in slot 4 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting ethernet 4/0

Interface    Pkts In   Chars In   Pkts Out  Chars Out     Punted     Dropped
Ethernet4/0    0          0        122      11490          4          0
```

The following is sample output from the **show pxf accounting** *null* command using a null interface in slot 0 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting null 0/0

Interface    Pkts In   Chars In   Pkts Out  Chars Out     Punted    Dropped
nu0/0          0          0          0          0       4932          0
```

The following is sample output from the **show pxf accounting** *pos* command using a Packet-over-SONET interface in slot 4 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting pos

Interface    Pkts In   Chars In   Pkts Out  Chars Out     Punted    Dropped
POS4/0          19       1064         0          0         44         0
```

The following is sample output from the **show pxf accounting** *serial* command using a serial interface in slot 5 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting serial 5/0

Interface    Pkts In   Chars In   Pkts Out  Chars Out     Punted    Dropped
Serial5/0          0          0          0          0          0       0
```

The following is sample output from the **show pxf accounting** *summary* command:

```
Router# show pxf accounting summary

            Pkts        Dropped   RP Processed        Ignored
           Total              0          48360              0

PXF Statistic:
Packets RP -> PXF:
    switch ip:                0
    switch raw:           30048360
    qos fastsend:             0
    qos enqueue:           1938
Total:                    30050298

Packets PXF -> RP:
    qos pkts:              1938
    fast pkts:            30000000
    drops:total               0
    punts:total           48360
      "    not IP            :      40572
      "    CEF no adjacency  :       7788
Total:                    30050298

Packets ignored:              0     |    ring space:
```

```
    shadow ring full:          0     |        shadow ring:          16384
    in ring full:              0     |        inring:                 968
    PXF inactive:              0

tx credits:             16230330     |    delayed credits:              0
holdq enqueues:                0     |    requeue drops:                0
interrupts:                40538     |    interrupt misses:          1947
interrupt packets:         53326
pending read bytes:            0

     Interface    Pkts In   Chars In   Pkts Out  Chars Out     Punted    Dropped
         Fa0/0          0          0   30000000 1740000000        970          0
         Et1/0          0          0          0          0      21309          0
         Et1/1          0          0          0          0          0          0
         Et1/2          0          0          0          0          0          0
         Et1/3          0          0          0          0          0          0
         Se2/0          0          0          0          0        963          0
         Se2/1          0          0          0          0          0          0
         Se2/2          0          0          0          0          0          0
         Se2/3          0          0          0          0          0          0
         Fa3/0          0          0          0          0        963          0
         PO4/0   30000000 1440000000          0          0        963          0
         AT5/0          0          0          0          0      23192          0
           Vi1          0          0          0          0          0          0
           Vt1          0          0          0          0          0          0
           Vi2          0          0          0          0          0          0
```

Related Commands

Command	Description
show pxf crash	Displays PXF crash information.
show pxf feature	Displays the PXF routing feature tables for enabled PXF features.
show pxf interface	Displays a summary of the interfaces in the router and the PXF features or capabilities enabled on these interfaces.

show pxf crash

To show PXF crash information, use the **show pxf crash** EXEC command.

show pxf crash

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following is sample output from the **show pxf crash** command:

```
Router# show pxf crash

      EX_Type = 0x80000000
      EX_ID(b0~3,16~17) = 0x00400
      CPU_EX_ID(b0~15) = 0x0004
      IHB_EX_Type(b0~5) = 0x00
      XRAM0(b0~13) = 0x00000
      XRAM1(b0~13) = 0x00000
      XRAM2(b0~13) = 0x00000
      XRAM3(b0~13) = 0x00000
      Pipeline:7FDEFD pdone[3210]:1F  17  17  1D

    ICM0(b4~13) = 0x00000  ICM1(b4~13) = 0x00000
    ICM2(b4~13) = 0x00010  ICM3(b4~13) = 0x00000
    LOCK0(b0~4) = 0x00000  LOCK1(b0~4) = 0x00000
    LOCK2(b0~4) = 0x00000  LOCK3(b0~4) = 0x00000
    CPU0/2: SW EX Type=0x00000000 LBUS EX Type=0x00000081 HW EX
    Type=0x00000400

    CPU:row=0x0 column=0x2 cpu=0x2
     PC:0000098E  LR:0000087F  CR:002C4C00
     r0:00000000  r1:8001CEA0  r2:80784390  r3:00000000
     r4:00005400  r5:80D3BA04  r6:80A7CA00  r7:00000004
     r8:00000000  r9:00000008 r10:80092324 r11:800A6200
    r12:00000033 r13:00000008 r14:00000000 r15:00000000
      misr1a:00000000 misr1bhi:00000000 misr1blo:00000000  misr2hi:00000000
     misr2lo:00000000  reserve:00000000  reserve:00000000  reserve:00000000
      sisr1a:01000040   sisr1b:00000000     irhi:4402200F     irlo:00000000
    cAll:C20DE822 DCD1:00020400 DCD2:00000002 CNTL:00000000
    TBuf intr 0:1111111F
    TBuf intr 1:020FFFF0
    TBuf intr 2:00003C80
```

```
TBuf intr 3:80000000
TBuf intr 4:00000400
Xram return:00000000
Icram return hi:80024E00
Icram return lo:800A4E00
TBuf addr 0:005E6800 TBuf sblock1 0:8078A374 TBuf sblock0 0:804FD600
TBuf addr 1:005E6800 TBuf sblock1 1:8078A374 TBuf sblock0 1:804FD600
TBuf addr 2:005E6800 TBuf sblock1 2:8078A374 TBuf sblock0 2:804FD600
TBuf addr 3:005E6800 TBuf sblock1 3:8078A374 TBuf sblock0 3:804FD600
TBuf addr 4:005E6800 TBuf sblock1 4:8078A374 TBuf sblock0 4:804FD600
TBuf addr 5:005E6800 TBuf sblock1 5:8078A374 TBuf sblock0 5:804FD600
TBuf addr 6:005E6800 TBuf sblock1 6:8078A374 TBuf sblock0 6:804FD600
TBuf addr 7:005E6800 TBuf sblock1 7:8078A374 TBuf sblock0 7:804FD600
```

show pxf feature cef

To display PXF routing feature tables for Cisco Express Forwarding (CEF), use the **show pxf feature cef** EXEC command.

show pxf feature cef *entry*

Syntax Description

entry	Display the PXF entry.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following is sample output from the **show pxf feature cef** command:

```
Router# show pxf feature cef entry

    Shadow 16-4-4-8 PXF Mtrie:
      41 leaves, 1968 leaf bytes, 15 nodes, 267000 node bytes
      5 invalidations
      46 prefix updates
      refcounts: 66746 leaf, 66720 node

    Prefix/Length        Refcount   Parent
    0.0.0.0/0           62282
    0.0.0.0/32          3           0.0.0.0/0
    171.69.12.128/27    34          0.0.0.0/0
    171.69.12.128/32    3           171.69.12.128/27
    171.69.12.129/32    3           171.69.12.128/27
    171.69.12.130/32    3           171.69.12.128/27
    171.69.12.131/32    3           171.69.12.128/27
    171.69.12.147/32    3           171.69.12.128/27
```

Related Commands

Command	Description
show pxf feature nat	Displays PXF routing feature tables for NAT.

show pxf feature nat

To display PXF routing tables for Network Address Translation (NAT), use the **show pxf feature nat** EXEC command.

show pxf feature nat [*entry* | *stat* | *tcp*]

Syntax Description

entry	Displays NAT information.
stat	Displays NAT processing information.
tcp	Displays NAT TCP logging information.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following is sample output from the **show pxf feature** command:

```
Router# show pxf feature nat 1

--- 171.69.12.175      192.168.0.129      ---                ---
--- 171.69.12.163      192.168.0.7        ---                ---
--- 171.69.12.161      192.168.0.13       ---                ---
--- 171.69.12.162      192.168.0.3        ---                ---
--- 171.69.12.165      192.168.0.8        ---                ---
--- 171.69.12.168      192.168.0.14       ---                ---
--- 171.69.12.170      192.168.0.12       ---                ---
--- 171.69.12.166      192.168.0.15       ---                ---
--- 171.69.12.164      192.168.0.16       ---                ---
```

Related Commands

Command	Description
show pxf feature cef	Displays PXF routing feature tables for CEF.

show pxf interface

To show a summary of the interfaces on the router and the PXF features or capabilities enabled on these interfaces, use the **show pxf interface** command.

show pxf interface

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following is sample output from the **show pxf interface** command:

```
Router# show pxf interface

 Intf  I/f #  Attributes
Fa0/0    3    Raw, Encap, QoS(Cr 0, Thrsh 2, Max 101)
Et1/0    4    Raw, Encap
Et1/1    5    Raw, Encap, QoS(Cr 0, Thrsh 2, Max 13)
Et1/2    6    Raw, Encap
Et1/3    7    Raw, Encap
Se2/0    8    Raw, Encap, QoS(Cr 0, Thrsh 2, Max 5)
Se2/1    9    Raw, Encap, QoS(Cr 0, Thrsh 2, Max 5)
Se2/2    10   Raw, Encap, QoS(Cr 0, Thrsh 2, Max 5)
Se2/3    11   Raw, Encap, QoS(Cr 0, Thrsh 2, Max 5)
Fa3/0    12   Raw, Encap
PO4/0    13   Raw, Encap
AT5/0    14   Raw, Encap
```

Related Commands

Command	Description
show pxf feature	Displays the PXF routing feature tables for enabled PXF features.

show route-map ipc

To display counts of the one-way route map IPC messages sent from the RP to the VIP when NetFlow policy routing is configured, use the **show route-map ipc** command in EXEC mode.

show route-map ipc

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

If you execute this command on the RP, the messages are shown as "Sent." If you execute this command on the VIP console, the IPC messages are shown as "Received."

Examples

The following is sample output of the **show route-map ipc** command when it is executed on the RP:

```
Router# show route-map ipc

Route-map RP IPC Config Updates Sent
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```

The following is sample output of the **show route-map ipc** command when it is executed on the VIP:

```
Router# show route-map ipc

Route-map LC IPC Config Updates Received
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```

Table 87 describes the significant fields shown in the output.

Table 87 show route-map ipc Field Descriptions

Field	Description
Route-map RP IPC Config Updates Sent	Indicates that IPC messages are being sent from the RP to the VIP.
Name:	Number of IPC messages sent about the name of the route map.
Match access-list:	Number of IPC messages sent about the access list.
Match length	Number of IPC messages sent about the length to match.
Set precedence:	Number of IPC messages sent about the precedence.
Set tos:	Number of IPC messages sent about the type of service (ToS).
Set nexthop:	Number of IPC messages sent about the next hop.
Set interface:	Number of IPC messages sent about the interface.
Set default nexthop:	Number of IPC messages sent about the default next hop.
Set default interface:	Number of IPC messages sent about the default interface.
Clean all:	Number of IPC messages sent about clearing the policy routing configuration from the VIP. When dCEF is disabled and reenabled, the configuration related to policy routing must be removed (cleaned) from the VIP before the new information is downloaded from the RP to the VIP.

show tag-switching atm-tdp bindings

To display the requested entries from the ATM LDP label bindings database, use the s**how tag-switching atm-tdp bindings** EXEC command.

show tag-switching atm-tdp bindings [*A.B.C.D* {*mask* | *length*}][**local-tag | remote-tag** *vpi vci*] [**neighbor atm** *slot/subslot/port*][**remote-tag** *vpi vci*]

Syntax Description

A.B.C.D	(Optional) Destination of the prefix.
mask	(Optional) Destination netmask prefix.
length	(Optional) Netmask length, in the range from 1 to 32.
local-tag *vpi vci*	(Optional) Matches locally assigned label values.
neighbor atm *slot/subslot/port*	(Optional) Matches labels assigned by a neighbor on the specified ATM interface.
remote-tag *vpi vci*	(Optional) Matches remotely assigned label values.

Defaults

Displays all database entries.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The display output can show the entire database or a subset of entries based on the prefix, the VC label value, or an assigning interface.

Examples

The following is sample output from this command:

```
Switch#  show tag-switching atm-tdp bindings

Destination: 13.13.13.6/32
Headend Router ATM1/0.1 (2 hops) 1/33 Active, VCD=8, CoS=available
Headend Router ATM1/0.1 (2 hops) 1/34 Active, VCD=9, CoS=standard
Headend Router ATM1/0.1 (2 hops) 1/35 Active, VCD=10, CoS=premium
Headend Router ATM1/0.1 (2 hops) 1/36 Active, VCD=11, CoS=control

Destination: 102.0.0.0/8
Headend Router ATM1/0.1 (1 hop) 1/37 Active, VCD=4, CoS=available
Headend Router ATM1/0.1 (1 hop) 1/34 Active, VCD=5, CoS=standard
Headend Router ATM1/0.1 (1 hop) 1/35 Active, VCD=6, CoS=premium
Headend Router ATM1/0.1 (1 hop) 1/36 Active, VCD=7, CoS=control

Destination: 13.0.0.18/32
Tailend Router ATM1/0.1 1/33 Active, VCD=8
```

Table 88 describes the significant fields in the sample command output shown above.

Table 88 show tag-switching atm-tdp bindings Field Descriptions

Field	Description
Destination:	Destination IP address or length of the netmask
Headend Router	VC type: • Headend—VC that originates at this router • Tailend—VC that terminates at this router
ATM1/0.1	ATM interface .
1/33	VPI/VCI.
Active	LVC state. Can be either of the following: • Active—Set up and working • Bindwait—Waiting for response

Related Commands

Command	Description
show tag-switching atm-tdp bindwait	Displays the number of bindings waiting for label assignments for a remote MPLS ATM switch.

show tag-switching atm-tdp bindwait

To display the number of bindings waiting for label assignments from a remote MPLS ATM switch, use the **show tag-switching atm-tdp bindwait** EXEC command.

show tag-switching atm-tdp bindwait

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Related Commands

Command	Description
show tag-switching atm-tdp bindings	Displays requested entries from the ATM LDP label binding database.

show tag-switching atm-tdp capability

To display the ATM LDP label capabilities, use the **show tag-switching atm-tdp capability** command in privileged EXEC mode.

show tag-switching atm-tdp capability

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.

Examples

The following example shows the display from the **show tag-switching atm-tdp capability** command:

```
Router> show tag-switching atm-tdp 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 89 describes the significant fields shown in the output.

Table 89 show tag-switching atm-tdp capability Field Descriptions

Field	Description
VPI Range	Minimum and maximum number of VPIs supported on this interface.
VCI Range	Minimum and maximum number of VCIs supported on this interface.

Table 89 show tag-switching atm-tdp capability Field Descriptions (continued)

Field	Description
Alloc Scheme	UNIDIR—Unidirectional capability indicates that the peer device 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 device allocates bindings in the even VCI space, and the other in the odd VCI space. The system with the lower LDP identifier will assign even-numbered VCIs. The negotiated allocation scheme is UNIDIR if and only if both peer devices have UNIDIR capability. Otherwise it is BIDIR.
Odd/Even Scheme	Indicates whether the local device or the peer device 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.
VC Merge	Indicates the type of VC merge support on this interface. IN—Indicates 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 output interface merge capability. OUT accepts the same values as the input merge side. The VC merge capability is meaningful only on ATM switches. It is not negotiated.
Negotiated	Set of options that both LDP peer devices have agreed to share on this interface. For example, the VPI or VCI allocation on either peer device remains within the negotiated ranges.
Local	Options supported locally on this interface.
Peer	Options supported by the remote LDP peer device on this interface.

Related Commands

Command	Description
tag-switching atm control-vc	Configures the VPI and VCI to be used for the initial link to the label switching peer device.
tag-switching atm vc-merge	Controls whether vc-merge (multipoint-to-point) is supported for unicast label VCs.
tag-switching atm vpi	Configures the range of values to use in the VPI field for label VCs.

show tag-switching atm-tdp summary

To display summary information on ATM label bindings, use the **show tag-switching atm-tdp summary** command in privileged EXEC mode.

show tag-switching atm-tdp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.

Examples

The following is sample output from the **show tag-switching atm-tdp summary** command:

```
Router> show tag-switching atm-tdp summary

Total number of destinations: 788

TC-ATM bindings summary
interface   total     active    bindwait  local     remote    other
ATM0/0/0    594       592       1         296       298       1
ATM0/0/1    590       589       0         294       296       1
ATM0/0/2    1179      1178      0         591       588       1
ATM0/0/3    1177      1176      0         592       585       1
ATM0/1/0    1182      1178      4         590       588       0
Waiting for bind on ATM0/0/0 10.21.0.0/24
```

Table 90 describes the significant fields shown in the output.

Table 90 show tag-switching atm-tdp summary Field Descriptions

Field	Description
Total number of destinations	The number of known destination address prefixes.
interface	The name of an interface that has associated ATM label bindings.
total	The total number of ATM labels on this interface.
active	The number of ATM labels in an “active” state that are ready to be used for data transfer.
bindwait	The number of bindings that are waiting for a label assignment from the neighbor LSR.
local	The number of ATM labels assigned by this LSR on this interface.
remote	The number of ATM labels assigned by the neighbor LSR on this interface.

Table 90 show tag-switching atm-tdp summary Field Descriptions (continued)

Field	Description
other	The number of ATM labels in a state other than “active” or “bindwait.”
Waiting for bind on ATM0/0/0	A list of the destination address prefixes (on a particular interface) that are waiting for ATM label assignment from the neighbor LSR.

Related Commands

Command	Description
show isis database verbose	Displays the requested entries from the ATM LDP label binding database.

show tag-switching cos-map

To display the QoS map used to assign a quantity of label VCs (LVCs) and an associated QoS of those LVCs, use the **show tag-switching cos-map** EXEC command in EXEC mode.

show tag-switching cos-map

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following example shows output from this command:

```
Router# show tag-switching cos-map

cos-map 2    class  tag-VC
             3      control
             2      control
             1      available
             0      available
```

Table 91 describes the significant fields shown in the output.

Table 91 show tag-switching cos-map Field Descriptions

Field	Description
cos-map	Configures a class map, which specifies how classes map to MPLS VCs when combined with a prefix map.
class	The IP precedence.
tag-VC	An ATM VC that is set up through ATM LSR label distribution procedures.

Related Commands

Command	Description
class (MPLS)	Configures an MPLS CoS map that specifies how classes map to LVCs when combined with a prefix map.
tag-switching cos-map	Creates a class map that specifies how classes map to LVCs when combined with a prefix map.

show tag-switching forwarding-table

The **show tag-switching forwarding-table** command is replaced by the **show mpls forwarding-table** command. See the **show mpls forwarding-table** command for more information.

show tag-switching forwarding vrf

The **show tag-switching forwarding vrf** command is replaced by the **show mpls forwarding-table** command. See the **show mpls forwarding-table** command for more information.

show tag-switching interfaces

The **show tag-switching interfaces** command is replaced by the **show mpls interfaces** command. See the **show mpls interfaces** command for more information.

show tag-switching prefix-map

To show the prefix map used to assign a QoS map to network prefixes matching a standard IP access list, use the **show tag-switching prefix-map** command in EXEC mode.

show tag-switching prefix-map [*prefix-map*]

Syntax Description

prefix-map	(Optional) Specifies the prefix-map number.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output from the **show tag-switching prefix-map** command:

```
Router# show tag-switching prefix-map

prefix-map 2 access-list 2 cos-map 2
```

Table 92 describes the significant fields shown in the output.

Table 92 show tag-switching prefix-map Field Description

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
tag-switching prefix-map	Displays the prefix map used to assign a QoS map to network prefixes matching a standard IP access list.

show tag-switching tdp bindings

To display the contents of the label information base (LIB), use the **show tag-switching tdp bindings** command in privileged EXEC mode.

show tag-switching tdp bindings [*network*{*mask* | *length*} [**longer-prefixes**]] [**local-tag** *tag* [**-** *tag*]] [**remote-tag** *tag* [**-** *tag*]] [**neighbor** *address*] [**local**]

Syntax Description

network	(Optional) Destination network number.
mask	(Optional) Network mask written as A.B.C.D.
length	(Optional) Mask length (1 to 32 characters).
longer-prefixes	(Optional) Selects any prefix that matches the *mask* with *length* value to 32.
local-tag *tag* **-** *tag*	(Optional) Displays entries matching local label values by this router. Use the **-** *tag* argument to indicate the label range.
remote-tag *tag* **-** *tag*	(Optional) Displays entries matching label values assigned by a neighbor router. Use the **-** *tag* argument to indicate the label range.
neighbor *address*	(Optional) Displays label bindings assigned by selected neighbor.
local	(Optional) Displays local label bindings.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.

Usage Guidelines

A request can specify that the entire database be shown, or it or can be limited to a subset of entries. A request to show a subset of entries can be based on the prefix, on input or output label values or ranges, or on the neighbor advertising the label.

Examples

The following is sample output from the **show tag-switching tdp bindings** command. This form of the command causes the contents of the entire LIB (TIB) to be displayed.

```
Router# show tag-switching tdp bindings

Matching entries:
  tib entry: 10.92.0.0/16, rev 28
        local binding:  tag: imp-null(1)
        remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
  tib entry: 10.102.0.0/16, rev 29
        local binding:  tag: 26
        remote binding: tsr: 172.27.32.29:0, tag: 26
  tib entry: 10.105.0.0/16, rev 30
        local binding:  tag: imp-null(1)
        remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
  tib entry: 10.205.0.0/16, rev 31
        local binding:  tag: imp-null(1)
        remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
```

```
tib entry: 10.211.0.7/32, rev 32
      local binding:  tag: 27
      remote binding: tsr: 172.27.32.29:0, tag: 28
tib entry: 10.220.0.7/32, rev 33
      local binding:  tag: 28
      remote binding: tsr: 172.27.32.29:0, tag: 29
tib entry: 99.101.0.0/16, rev 35
      local binding:  tag: imp-null(1)
      remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 100.101.0.0/16, rev 36
      local binding:  tag: 29
      remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 171.69.204.0/24, rev 37
      local binding:  tag: imp-null(1)
      remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 172.27.32.0/22, rev 38
      local binding:  tag: imp-null(1)
      remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 210.10.0.0/16, rev 39
      local binding:  tag: imp-null(1)
tib entry: 210.10.0.8/32, rev 40
      remote binding: tsr: 172.27.32.29:0, tag: 27
```

The following is sample output from the **show tag-switching tdp bindings 10.0.0.0 8 longer-prefixes neighbor 172.27.32.29** variant of the command; it displays labels learned from LSR (TSR) 172.27.32.29 for network 10.0.0.0 and any of its subnets. The use of the **neighbor** option suppresses the output of local labels and labels learned from other neighbors.

```
Router# show tag-switching tdp bindings 10.0.0.0 8 longer-prefixes neighbor 172.27.32.29

tib entry: 10.92.0.0/16, rev 28
      remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 10.102.0.0/16, rev 29
      remote binding: tsr: 172.27.32.29:0, tag: 26
tib entry: 10.105.0.0/16, rev 30
      remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 10.205.0.0/16, rev 31
      remote binding: tsr: 172.27.32.29:0, tag: imp-null(1)
tib entry: 10.211.0.7/32, rev 32
      remote binding: tsr: 172.27.32.29:0, tag: 28
tib entry: 10.220.0.7/32, rev 33
      remote binding: tsr: 172.27.32.29:0, tag: 29
```

Table 93 describes the significant fields in the output.

Table 93 show tag-switching tdp bindings Field Descriptions

Field	Description
tib entry	Indicates that the following lines are the LIB (TIB) entry for a particular destination (network/mask). The revision number is used internally to manage label distribution for this destination.
remote binding	A list of outgoing labels for this destination learned from other Label Switching Routers (LSRs). Each item on this list identifies the LSR from which the outgoing label was learned and the label itself. The LSR is identified by its LDP identifier.
imp-null	The implicit null label. This label value instructs the upstream router to pop the label entry off the label stack before forwarding the packet.

Related Commands

Command	Description
show mpls forwarding-table	Displays the contents of the LFIB.
show tag-switching tdp neighbors	Displays the status of LDP sessions.

show tag-switching tdp discovery

To display the status of the LDP discovery process, use the **show tag-switching tdp discovery** command in privileged EXEC mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.

Usage Guidelines

Status of the LDP discovery process means a list of interfaces over which LDP discovery is running.

Examples

The following is sample output from the **show tag-switching tdp discovery** command.

```
Router# show tag-switching tdp discovery

Local TDP Identifier:
    172.27.32.29:0
TDP Discovery Sources:
    Interfaces:
ATM0/0.1:       xmit/recv
ATM0/0.1:       xmit/rec
Ethernet4/0/1:  xmit/recv
Ethernet4/0/2:  xmit/recv
POS6/0/0:       xmit/recv
```

Table 94 describes the significant fields shown in the output.

Table 94 show tag-switching tdp discovery Field Descriptions

Field	Description
Local TDP Identifier	The LDP identifier for the local router. An LDP identifier is a 6-byte quantity displayed as an IP address:number. The Cisco convention is to use a router ID for the first 4 bytes of the LDP identifier, and integers starting with 0 for the final 2 bytes of the IP address:number.
Interfaces	Lists the interfaces engaging in LDP discovery activity. “xmit” indicates that the interface is sending LDP discovery hello packets; “recv” indicates that the interface is receiving LDP discovery hello packets.

Related Commands

Command	Description
show tag-switching tdp neighbors	Displays the status of LDP sessions.

show tag-switching tdp neighbors

To display the status of Label Distribution Protocol (LDP) sessions, use the **show tag-switching tdp neighbors** command in privileged EXEC mode.

show tag-switching tdp neighbors [*address* | *interface*] [**detail**]

Syntax Description

address	(Optional) The neighbor that has this IP address.
interface	(Optional) LDP neighbors accessible over this interface.
detail	(Optional) Displays information in long form.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.

Usage Guidelines

The neighbor information branch can give information about all LDP neighbors, or it can be limited to

- The neighbor with a specific IP address
- LDP neighbors known to be accessible over a specific interface

Examples

The following is sample output from the **show tag-switching tdp neighbors** command:

```
Router# show tag-switching tdp neighbors

Peer TDP Ident: 10.220.0.7:1; Local TDP Ident 172.27.32.29:1
        TCP connection: 10.220.0.7.711 - 172.27.32.29.11029
        State: Oper; PIEs sent/rcvd: 17477/17487; Downstream on demand
Up time: 01:03:00
TDP discovery sources:
          ATM0/0.1
Peer TDP Ident: 210.10.0.8:0; Local TDP Ident 172.27.32.29:0
        TCP connection: 210.10.0.8.11004 - 172.27.32.29.711
        State: Oper; PIEs sent/rcvd: 14656/14675; Downstream
Up time: 2d5h
        TDP discovery sources:
          Ethernet4/0/1
          Ethernet4/0/2
          POS6/0/0
        Addresses bound to peer TDP Ident:
          99.101.0.8      172.27.32.28    10.105.0.8      10.92.0.8
          10.205.0.8      210.10.0.8
```

Table 95 describes the significant fields shown in the output.

Table 95 show tag-switching tdp neighbors Field Descriptions

Field	Description
Peer TDP Ident	The LDP identifier of the neighbor (peer device) for this session.
Local TDP Ident	The LDP identifier for the local LSR (TSR) for this session.
TCP connection	The TCP connection used to support the LDP session. The format for displaying the TCP connection is as follows: *peer IP address.peer port* *local IP address.local port*
State	The state of the LDP session. Generally this is Oper (operational), but Transient is another possible state.
PIEs sent/rcvd	The number of LDP protocol information elements (PIEs) sent to and received from the session peer device. The count includes the transmission and receipt of periodic keepalive PIEs, which are required for maintenance of the LDP session.
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 device (subject to any configured access list restrictions).
Downstream on demand	Indicates that the downstream-on-demand method of label distribution is being used for this LDP session. When the downstream-on-demand method is used, an LSR advertises its locally assigned (incoming) labels to its LDP peer device only when the peer device asks for them.
Up time	The length of time the LDP session has existed.
TDP discovery sources	The sources of LDP discovery activity that led to the establishment of this LDP session.
Addresses bound to peer TDP Ident	The known interface addresses of the LDP session peer device. These are addresses that may appear as next hop addresses in the local routing table. They are used to maintain the label forwarding information base (LFIB).

Related Commands

Command	Description
show tag-switching tdp discovery	Displays the status of the LDP discovery process.

show tag-switching tdp parameters

To display available LDP (TDP) parameters, use the **show tag-switching tdp parameters** command in privileged EXEC mode.

show tag-switching tdp parameters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CT	This command was introduced.

Examples

The following is sample output from the **show tag-switching tdp parameters** command:

```
Router# show tag-switching tdp parameters

Protocol version: 1
 Downstream tag pool: min tag: 10; max_tag: 10000; reserved tags: 16
 Session hold time: 15 sec; keep alive interval: 5 sec
 Discovery hello: holdtime: 15 sec; interval: 5 sec
 Discovery directed hello: holdtime: 15 sec; interval: 5 sec
 Accepting directed hellos
```

Table 96 describes the significant fields shown in the output.

Table 96 show tag-switching tdp parameters Field Descriptions

Field	Description
Protocol version	Indicates the version of the LDP running on the platform.
Downstream tag pool	Describes the range of labels available for the platform to assign for label switching. The labels available run 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 to maintain an LDP session with an LDP peer device without receiving LDP traffic or an LDP keepalive from the peer device.
keep alive interval	Indicates the interval of time between consecutive transmission LDP keepalive messages to an LDP peer device.
Discovery hello	Indicates the amount of time 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 sending LDP hello messages to neighbors (interval).

Table 96 show tag-switching tdp parameters Field Descriptions (continued)

Field	Description
Discovery directed hello	Indicates the amount of time to remember that a neighbor platform wants an LDP session when the neighbor platform is not directly connected to the router and the neighbor platform has not sent an LDP hello message. The interval is known as hold time. Also indicates the time interval between the transmission of hello messages to a neighbor not directly connected to the router.
Accepting directed hellos	Indicates that the platform will accept and act on directed LDP hello messages. This field may not be present.

Related Commands

Command	Description
tag-switching tdp discovery	Configures the interval between transmission of LDP discovery hello messages.
tag-switching tdp holdtime	Enables LSP tunnel functionality on a device.

show tag-switching tsp-tunnels

The **show tag-switching tsp-tunnels** command is replaced by the **show mpls traffic-eng tunnels** command. See the **show mpls traffic-eng tunnels** command for more information.

show vlans

To view virtual LAN (VLAN) subinterfaces, use the **show vlans** privileged EXEC command.

show vlans

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.1(3)T	This command was modified to display traffic count on FastEthernet subinterfaces.

Examples

The following is sample output from the **show vlans** command:

```
RouterC7xxx# show vlans

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:   FastEthernet5/0.1

    Protocols Configured:   Address:              Received:        Transmitted:
            IP              56.0.0.3                    16               92129

Virtual LAN ID:  3 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:   Ethernet6/0/1.1

    Protocols Configured:   Address:              Received:        Transmitted:
            IP              36.0.0.3                  1558               1521

Virtual LAN ID:  4 (Inter Switch Link Encapsulation)

    vLAN Trunk Interface:   FastEthernet5/0.2

    Protocols Configured:   Address:              Received:        Transmitted:
            IP              76.0.0.3                     0                  7
```

The following is sample output from the **show vlans** command indicating a native VLAN and a bridged group:

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet1/0/2

 This is configured as native Vlan for the following interface(s) :
```

```
FastEthernet1/0/2

   Protocols Configured:   Address: Received:        Transmitted:

Virtual LAN ID:  100 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet1/0/2.1

   Protocols Configured:   Address: Received:        Transmitted:

        Bridging        Bridge Group 1 0                   0
```

Table 97 describes the significant fields shown in the output.

Table 97 show vlans Field Descriptions

Field	Description
Virtual LAN ID	Domain number of the VLAN.
vLAN Trunk Interface	Subinterface that carries the VLAN traffic.
Protocols Configured	Protocols configured on the VLAN.
Address	Network address.
Received	Packets received.
Transmitted	Packets sent.

show xtagatm cos-bandwidth-allocation xtagatm

To display information about QoS bandwidth allocation on extended MPLS ATM interfaces, use the **show xtagatm cos-bandwidth-allocation xtagatm** EXEC command.

show xtagatm cos-bandwidth-allocation xtagatm [**xtagatm** *interface number*]

Syntax Description

xtagatm *interface number*	(Optional) Specifies the XTagATM interface number.

Defaults

Available 50 percent, control 50 percent.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to display CoS bandwidth allocation information for the following CoS traffic categories:

- Available
- Standard
- Premium
- Control

Examples

The following example shows output from this command:

```
Router# show xtagatm cos-bandwidth-allocation xtagatm 123

CoSBandwidth allocation
available25%
standard25%
premium25%
control25%
```

show xtagatm cross-connect

To display information about the LSC view of the cross-connect table on the remotely controlled ATM switch, use the **show xtagatm cross-connect** EXEC command.

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 VPI/VCI on the specified interface.
descriptor *descriptor*	(Optional) Displays only connections with an endpoint on the interface with the specified physical descriptor.

Defaults

No default behavior or values.

Related Commands

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

Each connection is listed twice in the sample output from the **show xtagatm cross-connect** command under each interface that is linked by the connection. Connections are marked as -> (unidirectional traffic flow, into the first interface), <- (unidirectional traffic flow, away from the interface), or <-> (bidirectional).

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 98 describes the significant fields in the sample command output shown above.

Table 98 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 notation -> indicates an ingress endpoint, where traffic is only expected to be received into the switch; <- indicates an egress endpoint, where traffic is only expected to be sent from the interface; <-> indicates that traffic is expected to be both sent 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

A sample of the detailed command output provided for a single endpoint is as follows.

```
Router# show xtagatm cross-connect descriptor 12.1.0 1 42

Phys desc:   12.1.0
Interface:   n/a
Intf type:   switch control port
VPI/VCI:     1/42
X-Phys desc: 12.2.0
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 99 describes the significant fields in the sample command output shown above.

Table 99 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 MPLS ATM 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.
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

Table 99 show xtagatm cross-connect descriptor Field Descriptions (continued)

Field	Description
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

To display information about terminating VCs on extended MPLS ATM (XTagATM) interfaces, use the **show xtagatm vc** EXEC command.

show xtagatm vc [*vcd* [*interface*]]

Syntax Description

vcd	(Optional) Virtual circuit descriptor (virtual circuit number). If you specify the *vcd* argument, then detailed information about all VCs with that *vcd* appears. If you do not specify the *vcd* argument, a summary description of all VCs on all XTagATM interfaces appears.
interface	(Optional) Interface number. If you specify the *interface* and the *vcd* arguments, the single VC with the specified *vcd* on the specified *interface* is selected.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modifications
12.0(5)T	This command was introduced.

Usage Guidelines

The columns in the output 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 cross-connect** 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 100 describes the significant fields shown in the output.

Table 100 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.

tag-control-protocol vsi

To configure the use of VSI on a particular master control port, use the **tag-control-protocol vsi** interface configuration command. To disable VSI, use the **no** form of this command.

tag-control-protocol vsi [**id** *controller-id*] [**base-vc** *vpi vci*] [**slaves** *slave-count*] [**keepalive** *timeout*] [**retry** *timeout-count*]

no tag-control-protocol vsi [**id** *controller-id*] [**base-vc** *vpi vci*] [**slaves** *slave-count*] [**keepalive** *timeout*] [**retry** *timeout-count*]

Syntax Description

id *controller-id*	(Optional) Determines the value of the controller-id field present in the header of each VSI message. The default is 1.
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*
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).
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_count+1*. The default is 15 seconds.
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.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The command is only available on interfaces that can serve as a VSI master control port. We recommend 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**

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**

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:

```
interface atm 0/0
tag-control-protocol vsi 0 51
```

tag-switching advertise-tags

To control the distribution of locally assigned (incoming) labels via the Label Distribution Protocol (LDP), use the **tag-switching advertise-tags** command in global configuration mode. To disable label advertisement, use the **no** form of this command.

tag-switching advertise-tags [**for** *access-list-number* [**to** *access-list-number*]]

no tag-switching advertise-tags [**for** *access-list-number* [**to** *access-list-number*]]

Syntax Description

for *access-list-number*	(Optional) Specifies which destinations should have their labels advertised.
to *access-list-number*	(Optional) Specifies which LSR neighbors should receive label advertisements. An LSR is identified by the router ID that is the first 4 bytes of its 6-byte LDP identifier.

Defaults

The labels of all destinations are advertised to all LSR neighbors.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CT	This command was introduced.

Usage Guidelines

To enable the distribution of all locally assigned labels to all LDP neighbors, use the **tag-switching advertise-tags** command.

You can enter multiple **tag-switching advertise-tags** commands. Taken together, they determine how local labels are advertised.

Note This command has no effect for a TC-ATM interface. The effect is always as if the **tag-switching advertise-tags** command had been executed.

Examples

In the following example, the router is configured to advertise all locally assigned labels to all LDP neighbors. This is the default.

```
tag-switching advertise-tags
```

In the following example, the router is configured to advertise to all LDP neighbors labels for networks 10.101.0.0 and 10.221.0.0 only:

```
access-list 1 permit 10.101.0.0 0.0.255.255
```

```
access-list 4 permit 10.221.0.0 0.0.255.255
tag-switching advertise-tags for 1
tag-switching advertise-tags for 4
```

In the following example, the router is configured to advertise all labels to all LDP neighbors except neighbor 10.101.0.8:

```
access-list 1 permit any
access-list 2 deny  10.101.0.8
tag-switching advertise-tags
tag-switching advertise-tags for 1 to 2
```

tag-switching atm allocation-mode

To control the mode used for handling label binding requests on TC-ATM interfaces, use the **tag-switching atm allocation-mode** command in global configuration mode. To disable this feature, use the **no** form of this command.

tag-switching atm allocation-mode {**optimistic** | **conservative**}

no tag-switching atm allocation-mode {**optimistic** | **conservative**}

Syntax Description

optimistic	Label binding is returned immediately, and packets are discarded until the downstream setup is complete.
conservative	Label binding is delayed until the label VC has been set up downstream.

Defaults

The default is conservative.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CT	This command was introduced.

Examples

In the following example, the mode for handling binding requests is set to optimistic on a TC-ATM interface:

```
tag-switching atm allocation-mode optimistic
```

tag-switching atm control-vc

The **tag-switching atm control-vc** command is replaced by the **mpls atm control-vc** command. See the **mpls atm control-vc** command for more information.

tag-switching atm cos

To change the value of configured bandwidth allocation for QoS, use the **tag-switching atm cos** xtagatm interface configuration command.

tag-switching atm cos [**available** | **standard** | **premium** | **control**] *weight*

Syntax Description

available	(Optional) Specifies the weight for the **available** class. This is the lowest class priority.
standard	(Optional) Specifies the weight for the **standard** class. This is the next lowest class priority.
premium	(Optional) Specifies the weight for the **premium** class. This is the next highest class priority.
control	(Optional) Specifies the weight for the **control** class. This is the highest class priority.
weight	Specifies the total weight for all QoS traffic classes. This value ranges from 0 to 100.

Defaults

Available 50 percent, control 50 percent

Command Modes

xtagatm interface configuration

Command History

Release	Modifications
12.0(5)T	This command was introduced.

Examples

The following example shows output from this command:

```
tag-switching atm cos
interface XTagATM 0
ip unnumbered loopback0
no ip directed-broadcast
no ip route-cache cef
extended-port ATM1/0 bpx 10.2
tag-switching atm cos available 50
tag-switching atm cos control 50
tag-switching atm vpi 2-5
tag-switching ip
```

tag-switching atm disable-headend-vc

To remove all headend VCs from the MPLS LSC and disable its ability to function as an edge LSR, use the **tag-switching atm disable-headend-vc** command. To restore the headend VCs of the MPLS LSC and restores full edge LSR functionality, use the **no** form of this command.

tag-switching atm disable-headend-vc

no tag-switching atm disable-headend-vc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)DC	This command was introduced.

Usage Guidelines

The command prevents LSC from initiating headend VCs and hence reduces the number of VCs used in the network. The LSC can still terminate tailend VCs, if required.

Examples

In the following example, the MPLS LSC is disabled from acting like an edge LSR and therefore cannot create headend LVCs.

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

tag-switching atm maxhops

To limit the maximum hop count to a value you have specified, use the **tag-switching atm maxhops** command in global configuration mode. To ignore the hop count, use the **no** form of this command.

tag-switching atm maxhops [*number*]

no tag-switching atm maxhops

Syntax Description

number	(Optional) Maximum hop count.

Defaults

The default is 254.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CT	This command was introduced.

Usage Guidelines

When an ATM-LSR receives a BIND REQUEST, it does not send a BIND back if the value in the request is equal to the maxhops value. Instead, the ATM-LSR or LSR returns an error that specifies that the hop count has been reached.

When an ATM-LSR initiates a request for a label binding, it includes a parameter specifying the maximum number of hops that the request should travel before reaching the edge of the ATM Label Switching region. This is used to prevent forwarding loops in setting up label paths across the ATM region.

Examples

The following example sets the hop count limit to 2:

```
tag-switching atm maxhops 2
```

Related Commands

Command	Description
show isis database verbose	Displays the requested entries from the ATM LDP label binding database.

tag-switching atm multi-vc

To configure a router subinterface to create one or more tag-VCs over which packets of different classes are sent, use the **tag-switching atm multi-vc** command in ATM subinterface configuration submode. To disable this option, use the **no** form of this command.

tag-switching atm multi-vc

no tag-switching atm multi-vc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

ATM subinterface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This option is valid only on ATM MPLS subinterfaces.

Examples

The following commands configure interface a2/0/0.1 on the router for MPLS QoS multi-VC mode:

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
int a2/0/0.1 tag-switching
tag atm multi-vc
exit
exit
```

tag-switching atm vc-merge

To control whether vc-merge (multipoint-to-point) is supported for unicast label VCs, use the **tag-switching atm vc-merge** command in global configuration mode. To disable this feature, use the **no** form of this command.

tag-switching atm vc-merge

no tag-switching atm vc-merge

Syntax Description

This command has no arguments or keywords.

Defaults

The default is enabled if the hardware supports the ATM-VC merge capability.

Command Modes

Global configuration

Command History

Release	Modification
11.1 CT	This command was introduced.

Related Commands

Command	Description
show tag-switching atm-tdp capability	Displays the ATM LDP label capabilities.

tag-switching atm vpi

The **tag-switching atm vpi** command is replaced by the **mpls atm vpi** command. See the **mpls atm vpi** command for more information.

tag-switching atm vp-tunnel

To specify an interface or a subinterface as a VP tunnel, use the **tag-switching atm vp-tunnel** interface configuration command.

tag-switching atm vp-tunnel *vpi*

Syntax Description

vpi	Provides VPI value for the local end of the tunnel.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **tag-switching atm vp-tunnel** and **tag-switching atm vpi** commands are mutually exclusive.

This command is available on both extended MPLS ATM interfaces and on LC-ATM subinterfaces of ordinary router ATM interfaces. The command is not available on the LightStream 1010 device, where all subinterfaces are automatically VP tunnels.

On an XTagATM interface, the tunnel/nontunnel status and the VPI value to be used in case the XTagATM interface is a tunnel are normally learned from the switch through VSI interface discovery. Therefore, it is not necessary to use the **tag-switching atm vp-tunnel** command on an XTagATM interface in most applications.

Examples

The following example shows how to specify an MPLS subinterface VP tunnel with a VPI value of 4.

```
tag-switching atm vp-tunnel 4
```

tag-switching cos-map

To create a class map that specifies how classes map to label VCs when combined with a prefix map, use the **tag-switching cos-map** command in global configuration mode.

tag-switching cos-map *number*

Syntax Description

number	Unique number for a QoS map (from 1 to 255).

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

This example shows how to create a class map:

```
tag-switching cos-map 55
class 1 premium
exit
```

Related Commands

Command	Description
class (MPLS)	Configures an MPLS QoS map that specifies how classes map to LVCs when combined with a prefix map.
show tag-switching cos-map	Displays the QoS map used to assign quantity of LVC and associated QoS of those LVCs.

tag-switching ip (global configuration)

The **tag-switching ip** command is replaced by the **mpls ip** command. See the **mpls ip (global configuration)** command for more information.

tag-switching ip (interface configuration)

The **tag-switching ip** command is replaced by the **mpls ip** command. See the **mpls ip (interface configuration)** command for more information.

tag-switching ip default-route

The **tag-switching ip default-route** command is replaced by the **mpls ip default-route** command. See the **mpls ip default-route** command for more information.

tag-switching mtu

The **tag-switching mtu** command is replaced by the **mpls mtu** command. See the **mpls mtu** command for more information.

tag-switching prefix-map

To configure a router to use a specified QoS map when a label destination prefix matches the specified access list, use the **tag-switching prefix-map** command in ATM subinterface configuration submode.

tag-switching prefix-map *prefix-map* **access-list** *access-list* **cos-map** *cos-map*

Syntax Description

prefix-map	A unique number for a prefix map.
access-list *access list*	A unique number for a simple IP access list.
cos-map *cos-map*	A unique number for a CoS map.

Defaults

No default behavior or values.

Command Modes

ATM subinterface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This is a global command used to link an access list to a QoS map.

Examples

The following example links an access list to a QoS map:

```
tag-switching prefix-map 55 access-list 55 cos-map 55
```

Related Commands

Command	Description
show tag prefix-map	Displays the prefix map used to assign a QoS map to network prefixes matching a standard IP access list.

tag-switching request-tags for

To restrict the creation of LVCs through the use of access lists on the LSC or label edge router, use the **tag-switching request-tags for** global configuration command. To disable this feature, use the **no** form of this command.

tag-switching request-tags for *access-list*

no tag-switching request-tags for

Syntax Description

access-list	A named or numbered standard IP access list.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The command includes the following usage guidelines:

- You can specify either an access list number or name.
- When creating 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

In the following example, headend LVCs are prevented from being established from the LSC to all 198.x.x.x destinations. The following commands are added to the LSC configuration:

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

Related Commands

Command	Description
access list	Creates access lists.
ip access-list	Permits or denies access to IP addresses.

tag-switching tag-range downstream

The **tag-switching tag-range** command is replaced by the **mpls label range** command. See the **mpls label range** command for more information.

tag-switching tdp discovery

To configure the interval between transmission of LDP (TDP) discovery hello messages, or the hold time for a LDP transport connection, use the **tag-switching tdp discovery** command in global configuration mode.

tag-switching tdp discovery {**hello** | **directed hello**} {**holdtime** | **interval**} *seconds*

Syntax Description

hello	Configures the intervals and hold times for directly connected neighbors.
directed-hello	Configures the intervals and hold times for neighbors that are not directly connected (for example, LDP sessions that run through a LSP tunnel).
holdtime	The interval for which a connection stays up if no hello messages are received. The default is 15 seconds.
interval	The period between the sending of consecutive hello messages. The default is 5 seconds.
seconds	The hold time or interval.

Defaults

holdtime: 15 seconds
interval: 5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.1 CT	This command was introduced.

Examples

In the following example, the interval for which a connection stays up if no hello messages are received is set to 5 seconds:

```
tag-switching tdp discovery hello holdtime 5
```

Related Commands

Command	Description
show tag-switching tdp parameters	Displays available LDP parameters.
tag-switching tdp holdtime	Enables LSP tunnel functionality on a device.

tag-switching tdp holdtime

To enable LSP tunnel functionality on a device, use the **tag-switching tdp holdtime** command in global configuration mode.

tag-switching tdp holdtime *seconds*

Syntax Description

seconds	The time for which an LDP session is maintained in the absence of LDP messages from the session peer device.

Defaults

15 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.1 CT	This command was introduced.

Usage Guidelines

When an LDP session is initiated, the hold time is set to the lower of the values configured at the two ends.

Examples

In the following example, the hold time of LDP sessions is configured for 30 seconds:

```
tag-switching tdp holdtime 30
```

Related Commands

Command	Description
show tag-switching tdp parameters	Displays available LDP parameters.
tag-switching tdp discovery	Configures the interval between transmission of LDP discovery hello messages.

tag-switching tsp-tunnels (global configuration)

The **tag-switching tsp-tunnels** command is replaced by the **mpls traffic-eng tunnels** command. See the **mpls traffic-eng tunnels (global)** command for more information.

tag-switching tsp-tunnels (interface configuration)

The **tag-switching tsp-tunnels** command is replaced by the **mpls traffic-eng tunnels** command. See the **mpls traffic-eng tunnels (interface)** command for more information.

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 CEF 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.

Usage Guidelines

When this command is enabled on a GRE tunnel with both Cisco Express Forwarding (CEF) and NetFlow enabled, a NetFlow record is created for packets that are encapsulated by the tunnel.

Examples

The following example enables NetFlow record creation:

```
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 MPLS for traffic engineering, use the **tunnel mode mpls traffic-eng** interface configuration command. 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

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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

In the following example, the mode of the tunnel is set 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 calculation (if the tunnel is up).
tunnel mpls traffic-eng bandwidth	Configures the bandwidth required for an MPLS traffic engineering tunnel.
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 tag-switching

The **tunnel mode tag-switching** command is replaced by the **tunnel mode mpls traffic-eng** command. See the **tunnel mode mpls traffic-eng** command for more information.

tunnel mpls traffic-eng affinity

To configure an affinity (the properties the tunnel requires in its links) for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng affinity** interface configuration command. To disable this feature, 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.

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

In the following example, the affinity of the tunnel is set 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 announce

To specify that the 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** interface configuration command. 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.

Usage Guidelines

Currently, 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

In the following example, the instruction is given that if this tunnel is up, the IGP should use the tunnel in its enhanced SPF calculation:

```
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

In the following example, the instruction is given 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
```

In the following example, the tunnel requires 100 kBps of bandwidth:

```
Router(config-if)# tunnel mpls traffic-eng bandwidth 100
```

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 MPLS traffic engineering tunnel metric that the IGP enhanced SPF calculation uses, use the **tunnel mpls traffic-eng autoroute metric** interface configuration command. To disable this feature, 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.

Usage Guidelines

If you enter a relative value that causes the tunnel metric to be a negative number, the configuration is invalid.

Examples

The following example designates that the IGP enhanced SPF calculation will use MPLS traffic engineering tunnel metric negative 1:

```
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 bandwidth

To configure the bandwidth required for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng bandwidth** interface configuration command. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng bandwidth *bandwidth*

no tunnel mpls traffic-eng bandwidth *bandwidth*

Syntax Description

bandwidth	The bandwidth required for an MPLS traffic engineering tunnel. Bandwidth is specified in kBps.

Defaults

Default bandwidth is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the bandwidth required for an MPLS traffic engineering tunnel is 1000:

```
Router(config-if)# tunnel mpls traffic-eng bandwidth 1000 1Xwn
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays tunnel information.

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 between 1 and 1000000.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

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 load-share.

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 an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng path-option** interface configuration command. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng path-option *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*}} [**lockdown**]

no tunnel mpls traffic-eng path-option *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*}} [**lockdown**]

Syntax Description

number	When multiple path options are configured, lower numbered options are preferred.
dynamic	Path of the 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.
path-number	Path number of the IP explicit path that the tunnel uses with this option.
lockdown	(Optional) The LSP cannot be reoptimized.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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.

Examples

In the following example, the tunnel is configured 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 subcommand mode for IP explicit paths and creates or modifies the specified path.
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng priority	Configures the setup and reservation priority for an MPLS traffic engineering tunnel.

tunnel mpls traffic-eng priority

To configure the setup and reservation priority for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng priority** interface configuration command. To disable this feature, 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.

Usage Guidelines

When an 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

In the following example, a tunnel is configured 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 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.

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 the configuration of a two-hop tunnel. The first hop router/switch is 82.0.0.2, and the second and last hop is router/switch 81.0.0.2.

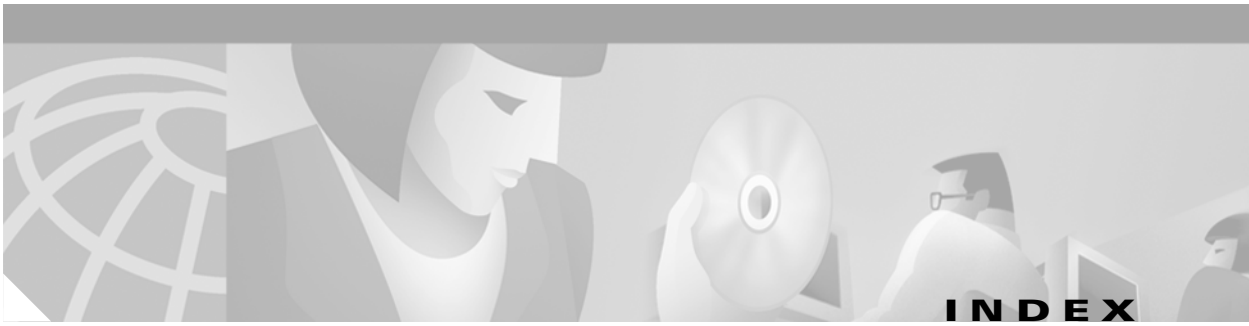
```
interface tunnel 5

tunnel mode tag-switching
ip unnumbered e0/1
  tunnel tsp-hop 1 82.0.0.2
  tunnel tsp-hop 2 81.0.0.2 lasthop
```

Related Commands

Command	Description
tunnel mode mpls traffic-eng	Sets the encapsulation mode of the tunnel to label switching.

Index



Symbols

<cr> xv
? command xiv

A

access-list rate-limit command XR-3
access lists, creating XR-433
addresses, exchanging XR-201
address-family command XR-5
affinity, configuring XR-480
append-after command XR-7
ARP table
  LANE
    dynamic entries, clearing XR-33
ATM
  interface XR-108
  interface, creating XR-61
  interface information, displaying XR-245
  LC encapsulation XR-64
  MPLS subinterface XR-461
  subinterface XR-461
  virtual circuit XR-429
atm-address command XR-8
attribute flags, setting XR-175

B

bandwidth
  changing XR-458
  link threshold, setting XR-176
  required bandwidth, configuring XR-485
  time and length for RSVP messages, setting XR-178
  XTagATM, displaying on XR-445
bgp default route-target filter command XR-9
BGP neighbor connections XR-267
bgp scan-time command XR-10
bit settings XR-16

C

cable bundle command XR-12
cable helper-address command XR-14
cache command XR-15
CAR (committed access rate)
  CAR policies, configuring XR-207
carriage return (<cr>) xv
cautions, usage in text x
cell rate XR-247
changed information in this release ix
cidr-only XR-267
Cisco 7500 series routers, subinterface numbers XR-61
Cisco IOS configuration changes, saving xviii
Cisco LightStream 1010 ATM switch, subinterface XR-158
class (MPLS) command XR-16
clean vlan mapping command XR-40
clear adjacency command XR-18
clear atm vc command XR-19
clear cef linecard command XR-21
clear ip cef event-log command XR-23
clear ip cef inconsistency command XR-24
clear ip cef prefix-statistics command XR-25
clear ip flow stats command XR-26
clear ip mds command XR-27

clear ip mds forwarding command XR-29
clear ip mroute command XR-30
clear ip pim interface count command XR-31
clear ip route vrf command XR-32
clear lane le-arp command XR-33
clear lane server command XR-35
clear mpoa client cache command XR-37
clear mpoa server cache command XR-38
clear vlan command XR-39
client-atm-address name command XR-41
command modes, understanding xiii to xiv
commands
  context-sensitive help for abbreviating xiv
  default form, using xvii
  no form, using xvii
command syntax
  conventions ix
  displaying (example) xv
community-list XR-267
configurations, saving xviii
connections
  TCP and BGP XR-267
cos-map, viewing XR-429
cos-map function XR-16, XR-429
cross-connects
  table, displaying XR-446
cross-connects, displaying XR-245, XR-264

D

DCAR (Distributed CAR) policies, configuring XR-207
default-name command XR-43
default RD XR-330
documentation
  conventions ix
  feedback, providing xi
  modules v to vii
  online, accessing x
  ordering xi
Documentation CD-ROM x
documents and resources, supporting viii
dynamic label switching, enabling XR-161
dynamic routing protocols XR-107

E

edge LSR, disabling XR-459
enabled command XR-45
encapsulation dot1q command XR-47
encapsulation isl command XR-48
encapsulation sde command XR-49
encapsulation tr-isl trbrf-vlan command XR-50
exit-address-family command XR-51
explicit paths, displaying XR-138
export destination command XR-52
export map command XR-54
extended-port command XR-56

F

family submode XR-51
Feature Navigator
  See platforms, supported
filtering output, show and more commands xviii
flap-statistics XR-267
flood
  flooded records, displaying XR-336
  interval, setting XR-179
flow switching
  See switching
forwarding table XR-32

H

hardware platforms
  See platforms, supported
headend LVC, disabling XR-459

help command xiv
holding-time command XR-58

I

IGP (Interior Gateway Protocol)
  administrative weight of link, overriding XR-173
  announced tunnels, displaying XR-376
  neighbors, displaying XR-384
IGRP (Interior Gateway Routing Protocol) XR-325
implicit-null, signaling messages XR-188
import map command XR-59
InBytes XR-227
index command XR-60
indexes, master viii
ingress XR-247
interface atm command XR-61
interface configuration mode, summary of xiv
interface fastethernet command XR-62
interfaces
  creating XR-158
  dynamic label switching, enabling XR-161
  MTU size, setting XR-169
  VPI range, assigning XR-160
interface XTagATM command XR-64
IP
  access lists XR-325
  addresses
    explicit paths, specifying XR-206
IP addresses
  explicit paths, displaying XR-296
ip cache-invalidate-delay command XR-65
ip cef accounting command XR-69
ip cef command XR-67
ip cef linecard ipc memory command XR-71
ip cef load-sharing algorithm command XR-72
ip cef table adjacency-prefix override command XR-74, XR-76
ip cef table consistency-check XR-77
ip cef table event-log command XR-79
ip cef table resolution-timer XR-81
ip cef traffic-statistics command XR-82
ip dhcp relay information option XR-84
ip explicit-path command XR-85
IP explicit paths, creating XR-85
IP explicit paths, modifying XR-85
ip flow-aggregation cache command XR-86
ip flow-cache entries command XR-87
ip flow-export command XR-89
ip flow-export source command XR-91
ip load-sharing command XR-93
ip mroute-cache command XR-95
IP multicast routing
  enabling XR-97
  fast-switching cache, displaying XR-300
  IP multicast routing table
    clearing XR-30
    displaying XR-309
  MDS
    enabling on interface XR-95
    interface status, displaying XR-304
    line card packet counts, clearing XR-31
    line card packet counts, displaying XR-305
    MFIB table, displaying XR-302
    MFIB table summary, displaying XR-307
    packet statistics, displaying XR-261
  PIM
    information, displaying XR-321
  RPF XR-309
ip multicast-routing command XR-97
ip route-cache command XR-98
ip route-cache policy command XR-105
ip route vrf command XR-106
IPv4 packets
  forwarding XR-161
  MTU size, setting XR-169
ip vrf command XR-109
ip vrf forwarding command XR-108

IS-IS (Intermediate System-To-Intermediate System)
adjacency changes, displaying XR-335
information about the database, displaying XR-332
information about tunnels, displaying XR-338
link information into database, flooding XR-172

K

keepalive-lifetime command XR-110
keepalive-time command XR-111

L

label forwarding information base, displaying XR-369
labels
distribution, enabling XR-163
free local labels, displaying XR-375
specifying the range for local labels XR-167
LANE
ATM addresses
automatic assignment XR-112
configuration server XR-112
fixed assignment XR-128
manual assignment XR-122
templates, ESI XR-115
templates, prefix XR-115
broadcast-and-unknown server
ATM address, manually specifying XR-114
different address to client, providing XR-114
client
address to database, adding XR-41
ATM address XR-117
emulated LAN exiting and rejoining XR-19
one per subinterface XR-116
subinterface, activating XR-116
configuration server
ATM address, assigning XR-112
ATM address, identifying server and client XR-122
ATM address, specifying XR-122
default LAN name in configuration server database XR-43
emulated LAN
client exiting and rejoining XR-19
client to join new, forcing XR-35
one per subinterface XR-116
LE ARP table
entries, clearing XR-19, XR-33
LECS
list of LECS addresses, specifying XR-131
MPOA
ELAN ID XR-196
simple LANE service replication XR-199
VCCs
data direct XR-119
lane auto-config-atm-address command XR-112
lane bus-atm-address command XR-114
lane client-atm-address command XR-117
lane client command XR-116
lane client flush command XR-119
lane client mpoa client name command XR-120
lane client mpoa server name command XR-121
lane config-atm-address command XR-122
lane config database command XR-124
lane database command XR-126
lane fixed-config-atm-address command XR-128
lane fssrp command XR-130
lane global-lecs-address command XR-131
lane le-arp command XR-132
lane server-atm-address command XR-134
lane server-bus command XR-136
LC-ATM encapsulation XR-64
LC-ATM interface
L VCs, preventing XR-161
learned routes XR-211
LE ARP table
dynamic entries, clearing XR-33
link information

available links, displaying XR-319
local, displaying XR-388
summary, displaying XR-382
list command XR-138
LocPrf XR-268, XR-269
logging
LSP events XR-182
traffic engineering tunnel events XR-183
loopback message XR-227
LSAs, displaying opaque LSAs XR-317
LSPs (link-state packets)
checking for better LSPs XR-186
LSP events, logging XR-182
LVC (label switched controlled virtual circuit) XR-429, XR-461, XR-465
active state XR-423
bindwait state XR-423
quantity, assigning XR-429

M

mask destination command XR-139
masks, specifying XR-32, XR-106, XR-267
mask source command XR-140
maximum routes command XR-141
MDS
See IP multicast routing, MDS
MEMD buffer XR-266
metric-style narrow command XR-143
metric-style transition command XR-144
metric-style wide command XR-145
MIB, descriptions online viii
MLSP (Multilayer Switching Protocol) XR-171
mls rp ip command XR-147
mls rp ip multicast command XR-148
mls rp ip multicast management-interface command XR-149
mls rp ipx (global) command XR-151
mls rp ipx (interface) command XR-152
mls rp locate ipx command XR-153
mls rp management-interface command XR-154
mls rp nde-address command XR-155
mls rp vlan-id command XR-156
mls rp vtp-domain command XR-157
modes
See command modes
mpls atm control-vc command XR-158
mpls atm vpi command XR-160
mpls ip (global configuration) command XR-161
mpls ip (interface configuration) command XR-162
mpls ip default-route command XR-163
mpls ip propagate-ttl command XR-164
mpls ip ttl-expiration pop command XR-165
mpls label range command XR-167
mpls mtu command XR-169
mpls netflow egress command XR-171
mpls traffic-eng administrative-weight command XR-173
mpls traffic-eng area XR-174
mpls traffic-eng area command XR-174
mpls traffic-eng attribute-flags command XR-175
mpls traffic-eng command XR-172
mpls traffic-eng flooding thresholds command XR-176
mpls traffic-eng link-management timers bandwidth-hold command XR-178
mpls traffic-eng link-management timers periodic-flooding command XR-179
mpls traffic-eng link timers bandwidth-hold command XR-180
mpls traffic-eng link timers periodic-flooding command XR-181
mpls traffic-eng logging lsp command XR-182
mpls traffic-eng logging tunnel command XR-183
mpls traffic-eng reoptimize command XR-184
mpls traffic-eng reoptimize events command XR-185
mpls traffic-eng reoptimize timers frequency command XR-186
mpls traffic-eng router-id command XR-187
mpls traffic-eng signaling advertise implicit-null command XR-188

mpls traffic-eng signalling advertise implicit-null command XR-188
mpls traffic-eng tunnels (configuration) command XR-189
mpls traffic-eng tunnels (interface) command XR-190
MPOA (Multiprotocol over ATM)
LANE client XR-196
mpoa client config name command XR-191
mpoa client name command XR-192
mpoa server config name command XR-193
mpoa server name command XR-194
mpoa server name trigger ip-address command XR-195
MTU (maximum transmission unit)
specifying XR-169
multicast distributed switching
See IP multicast routing, MDS
multicast MLSP
management interface XR-149
Multilayer Switching Protocol
See MLSP
multi-VC mode XR-461

N

name elan-id command XR-196
name local-seg-id command XR-197
name preempt command XR-198
name server-atm-address command XR-199
neighbor activate command XR-201
neighbor allowas-in command XR-202
neighbor as-override command XR-204
NetFlow switching
exporting cache entries XR-89
flow switching XR-89
network-id command XR-205
new information in this release ix
next-address command XR-206
next hop gateway address XR-106, XR-268, XR-269
NLRI (Network Layer Reachability Information) XR-267
notes, usage in text x

O

OSPF (Open Shortest Path First) XR-325
traffic engineering, flooding XR-174
OutBytes XR-227

P

packets
forwarding XR-165
input XR-227
output XR-227
rerouting XR-107
setting the MTU size XR-169
paths
index, inserting or modifying XR-60
index number, inserting after XR-7
path options, configuring XR-488
peer-group XR-267
platforms, supported
Feature Navigator, identify using xix
release notes, identify using xix
precedence assignments XR-16
prefix XR-106
prefix map XR-433
privileged EXEC mode, summary of xiv
process name XR-269, XR-324
prompts, system xiv

Q

QoS (quality of service)
bandwidth, displaying XR-445
configuring bandwidth for XR-458
maps XR-433
question mark (?) command xiv

R

rate-limit command XR-207
rate queue XR-227
rd command XR-210
release notes
  See platforms, supported
reoptimization
  events, turning on XR-185
  traffic engineering tunnels, forcing XR-184
reservation priority, configuring XR-489
Reverse Path Forwarding (RPF) XR-309
RFC
  full text, obtaining viii
ROM monitor mode, summary of xiv
route distinguisher XR-330
router identifier XR-187
routers, protocol information XR-323
router subinterface XR-461
routes
  filtering XR-59
  removing XR-32
route-target, configuring XR-211
route-target command XR-211
routing table XR-106
RPF (Reverse Path Forwarding) XR-309
RSVP (Resource Reservation Protocol)
  how long bandwidth is held, setting XR-178
  terminal point information, displaying XR-327

S

session number XR-254
set ip next-hop verify-availability command XR-213
set mpls experimental command XR-215
set ospf router-id command XR-216
setup priority, configuring XR-489
shortcut-frame-count command XR-221
shortcut-frame-time command XR-222
show adjacency command XR-223
show atm vc command XR-225
show cable bundle command XR-228
show cef drop command XR-229
show cef events command XR-231
show cef interface command XR-233
show cef interface policy-statistics command XR-237
show cef linecard command XR-239
show cef not-cef-switched command XR-242
show cef timers command XR-244
show controllers vsi control-interface command XR-245
show controllers vsi descriptor command XR-246
show controllers vsi session command XR-248
show controllers vsi status command XR-252
show controllers vsi traffic command XR-254
show controllers XTagATM command XR-258
show interface stats command XR-261
show interface XTagATM command XR-263
show ip bgp vpnv4 command XR-267
show ip cache command XR-270
show ip cache flow aggregation command XR-280
show ip cache flow command XR-273
show ip cef adjacency command XR-287
show ip cef command XR-283
show ip cef events command XR-289
show ip cef exact-route command XR-291
show ip cef inconsistency command XR-292
show ip cef traffic prefix-length command XR-294
show ip explicit-paths command XR-296
show ip flow export command XR-298
show ip mcache command XR-300
show ip mds forwarding command XR-302
show ip mds interface command XR-304
show ip mds stats command XR-305
show ip mds summary command XR-307
show ip mroute command XR-309
show ip ospf database opaque-area command XR-317
show ip ospf mpls traffic-eng command XR-319
show ip pim interface command XR-321

show ip protocols vrf command XR-323
show ip route vrf command XR-325
show ip rsvp host command XR-327
show ip vrf command XR-329
show isis database verbose command XR-332
show isis mpls traffic-eng adjacency-log command XR-335
show isis mpls traffic-eng advertisements command XR-336
show isis mpls traffic-eng tunnel command XR-338
show lane bus command XR-342
show lane client command XR-344
show lane command XR-339
show lane config command XR-348
show lane database command XR-350
show lane default-atm-addresses command XR-352
show lane le-arp command XR-354
show lane server command XR-356
show mls rp command XR-359
show mls rp interface command XR-361
show mls rp ip multicast command XR-362
show mls rp ipx command XR-365
show mls rp vtp-domain command XR-367
show mpls forwarding-table command XR-369
show mpls interfaces command XR-372
show mpls label range command XR-375
show mpls traffic-eng autoroute command XR-376
show mpls traffic-eng link-management admission-control command XR-378
show mpls traffic-eng link-management advertisements command XR-380
show mpls traffic-eng link-management bandwidth-allocation command XR-382
show mpls traffic-eng link-management igp-neighbors command XR-384
show mpls traffic-eng link-management interfaces command XR-386
show mpls traffic-eng link-management summary command XR-388
show mpls traffic-eng topology command XR-390
show mpls traffic-eng topology path command XR-392
show mpls traffic-eng tunnels command XR-394
show mpls traffic-eng tunnels summary command XR-397
show mpoa client cache command XR-401
show mpoa client command XR-399
show mpoa client statistics command XR-403
show mpoa default-atm-addresses command XR-404
show mpoa server cache command XR-408
show mpoa server command XR-406
show mpoa server statistics command XR-410
show pxf accounting command XR-412
show pxf crash command XR-415
show pxf feature cef command XR-417
show pxf feature nat command XR-418
show pxf interface command XR-419
show route-map ipc command XR-420
show tag-switching atm-tdp bindings command XR-422
show tag-switching atm-tdp bindwait command XR-424
show tag-switching atm-tdp capability command XR-425
show tag-switching atm-tdp summary command XR-427
show tag-switching cos-map command XR-429
show tag-switching forwarding-table command XR-430
show tag-switching forwarding vrf command XR-431
show tag-switching interfaces command XR-432
show tag-switching prefix-map command XR-433
show tag-switching tdp bindings command XR-434
show tag-switching tdp discovery command XR-437
show tag-switching tdp neighbors command XR-438
show tag-switching tdp parameters command XR-440
show tag-switching tsp-tunnels command XR-442
show vlans command XR-443
show xtagatm cos-bandwidth-allocation XTagATM command XR-445
show xtagatm cross-connect command XR-446
show xtagatm vc command XR-450
signaling
  device, enabling XR-189
  interface, enabling XR-190
static routes XR-32, XR-106, XR-107, XR-325
subinterface XR-461

supernet entries XR-325
switching
  flow switching XR-89

T

Tab key, command completion xiv
tag-control-protocol vsi command XR-452
tag-switching advertise-tags command XR-454
tag-switching atm allocation-mode command XR-456
tag-switching atm cos command XR-458
tag-switching atm disable-headend-vc command XR-459
tag-switching atm maxhops command XR-460
tag-switching atm multi-vc command XR-461
tag-switching atm vc-merge command XR-462
tag-switching atm vp-tunnel command XR-464
tag-switching cos-map command XR-465
tag-switching ip (global configuration) command XR-466
tag-switching ip (interface configuration) command XR-467
tag-switching ip default-route command XR-468
tag-switching mtu command XR-469
tag-switching prefix-map command XR-470
tag-switching request-tags for command XR-471
tag-switching tag-range downstream command XR-472
tag-switching tdp discovery command XR-473
tag-switching tdp holdtime command XR-474
tag-switching tsp-tunnels (global configuration) command XR-475
tag-switching tsp-tunnels (interface configuration) command XR-476
tag-VC XR-429
TCP connections XR-267
time to live
  expired packets XR-165
TLVs (type, length, and value objects)
  new style, generating and accepting XR-145
  old style, generating and accepting XR-143
  old style and new style, generating and accepting XR-144
topology
  global topology, displaying XR-390
trap filter XR-251
tunnel flow egress-records command XR-477
tunnel interface XR-64
tunnel mode mpls traffic-eng command XR-478
tunnel mode tag-switching command XR-479
tunnel mpls traffic-eng affinity command XR-480
tunnel mpls traffic-eng autoroute announce command XR-482
tunnel mpls traffic-eng autoroute metric command XR-483
tunnel mpls traffic-eng bandwidth command XR-485
tunnel mpls traffic-eng load-share command XR-486
tunnel mpls traffic-eng path-option command XR-488
tunnel mpls traffic-eng priority command XR-489
tunnels
  information about tunnels, displaying XR-394
  local admittance XR-378
  mode, setting XR-478
  required bandwidth, configuring XR-485
  setup and reservation priority, configuring XR-489
  summary information, displaying XR-397
  tunnel metric, specifying XR-483
tunnel tsp-hop command XR-491

U

user EXEC mode, summary of xiv

V

virtual channel identifier, specifying XR-158
VLANs (virtual LANs), monitoring XR-443
VPI (virtual path identifier)
  creating XR-158
  values, specifying XR-160
VPN (Virtual Private Network)
  address information XR-267
  extended community XR-211

VPNv4 information. displaying XR-268
VP tunnel, specifying XR-464
VRF (VPN routing/forwarding instance)
  configuring XR-109
  importing a route map XR-109
  routing table XR-109
  specifying name XR-330
  up/down status XR-330
VSI (Virtual Switch Interface)
  configuring XR-452
  descriptor string XR-56
  sessions, defining XR-248
  sessions, displaying XR-248
  status, displaying XR-252
  traffic information, displaying XR-254

X

XtagATM (extended tag ATM)
  associating with a switch XR-56
  information, displaying XR-258
  interfaces, configuring XR-64
  VCs, displaying XR-450